L Number	Hits	Search Text	DB	Time stamp
1	9701	standby with power	USPAT	2004/04/27 07:58
2	3	standby with power with screen with saver	USPAT	2004/04/27 07:59
3	69	power with screen with saver	USPAT	2004/04/27 08:02
4	18	power with screen with saver and password	USPAT	2004/04/27 08:43
5	1		USPAT	2004/04/27 08:11
6	1		USPAT	2004/04/27 08:11
7	1		USPAT	2004/04/27 08:13
8	1		USPAT	2004/04/27 08:13
9	9	wireless with keyboard with smart$4	USPAT	2004/04/27 08:44
10	32	keyboard with smartcard	USPAT	2004/04/27 09:40
11	1693	713/200,202.ccls.	USPAT	2004/04/27 09:41
12	847	713/200,202.ccls. and control$4 with computer	USPAT	2004/04/27 09:41
13	178	713/200,202.ccls. and control$4 with computer same password	USPAT	2004/04/27 09:42
16	18	713/200,202.ccls. and remote with control$4 with computer same password	USPAT	2004/04/27 10:09
19	1		USPAT	2004/04/27 09:58
20	4018	wireless adj network	USPAT	2004/04/27 10:09
21	157	(wireless adj network).ti.	USPAT	2004/04/27 10:10
-	146	"wireless mouse"	USPAT	2003/12/15 14:59
-	166	"computer remote control"	USPAT	2003/12/15 14:59
-	13	"computer remote control" and password	USPAT	2003/12/15 15:04
-	4	computer with (remot$2 adj control$4) with password	USPAT	2003/12/15 15:06
-	2731	computer with (remot$2 adj control$4)	USPAT	2003/12/15 15:06
-	325	computer with (remote adj controller)	USPAT	2003/12/15 15:11
-	497	"screen saver"	USPAT	2003/12/15 15:12
-	110	"screen saver" and "remote control"	USPAT	2003/12/15 15:17
-	1605	x10	USPAT	2003/12/15 15:17
-	14	x10 with remote with control	USPAT	2003/12/15 15:19
-	33	"5960085"	USPAT	2003/12/15 15:26
-	43	713/200.ccls. and "remote control"	USPAT	2003/12/15 15:30
-	14	713/202.ccls. and "remote control"	USPAT	2003/12/15 15:30
-	6	(US-4578674-$ or US-4754268-$ or US-5844552-$ or US-5471190-$ or US-5198806-$ or US-5960085-$).did.	USPAT	2003/12/16 08:47
-	1	((US-4578674-$ or US-4754268-$ or US-5844552-$ or US-5471190-$ or US-5198806-$ or US-5960085-$).did.) and windows	USPAT	2003/12/16 08:47
-	6	(US-4578674-$ or US-4754268-$ or US-5844552-$ or US-5471190-$ or US-5198806-$ or US-5960085-$).did.	USPAT	2003/12/16 08:47

-	1	((US-4578674-$ or US-4754268-$ or US-5844552-$ or US-5471190-$ or US-5198806-$ or US-5960085-$).did.) and encrypt$4	USPAT	2003/12/16 08:47
-	2	hong with sam with kim	USPAT	2004/04/26 15:42
-	142508	wireless keyboard	USPAT	2004/04/26 15:42
-	250	wireless adj keyboard	USPAT	2004/04/27 07:58
-	1	4313227.pn.	USPAT	2004/04/26 16:22
-	1		USPAT	2004/04/26 16:29
-	1		USPAT	2004/04/26 16:29
-	1		USPAT	2004/04/26 16:29
-	1		USPAT	2004/04/26 16:30
-	1		USPAT	2004/04/26 16:30
-	1		USPAT	2004/04/26 16:30
-	1		USPAT	2004/04/26 16:30
-	1		USPAT	2004/04/26 16:30
-	1		USPAT	2004/04/26 16:30

United States Patent [19]

Acampora et al.

[11] **Patent Number: 4,789,983**

[45] **Date of Patent: Dec. 6, 1988**

[54] **WIRELESS NETWORK FOR WIDEBAND INDOOR COMMUNICATIONS**

[75] Inventors: **Anthony Acampora**, Freehold; **Jack H. Winters**, Middletown, both of N.J.

[73] Assignee: **American Telephone and Telegraph Co., AT&T Bell Laboratories**, Murray Hill, N.J.

[21] Appl. No.: **22,255**

[22] Filed: **Mar. 5, 1987**

[51] **Int. Cl.**[4] **H04J 3/14**

[52] **U.S. Cl.** **370/96**; 370/84

[58] **Field of Search** 370/94, 95, 96, 109, 370/29, 13.1, 17, 97, 84; 379/58, 61, 63; 371/5

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,251,865	2/1981	Moore et al.	370/96
4,301,533	11/1981	Acampora et al.	370/104
4,309,764	1/1982	Acampora	370/83
4,398,289	8/1983	Schoute	370/94
4,606,044	8/1986	Kudo	370/84
4,692,919	9/1987	West, Jr.	370/96
4,742,514	5/1988	Goode et al.	370/97

OTHER PUBLICATIONS

Komura et al., Japan Telecomm. Rev., Quarterly, vol. 15, No. 4, 1973, pp. 257–261.

Acampora, BSTJ, vol. 58, No. 9, Nov. 1979, pp. 2097–2111.

Gfeller, IBM Discl. Bul, vol. 24, No. 8, Jan. 1982, pp. 4043–4046.

Acampora, IEEE Jrnl on SAC, vol. SAC-1, Jan. 1983, pp. 133–142.

Acampora et al., IEEE Communications Magazine, vol. 22, No. 8, Aug. 1984, pp. 12–21.

Mednick, Globecom '85, New Orleans, La., vol. 1, pp. 15.2.1 to 15.2.6.

Yen et al., Globecom '85, New Orleans, La., vol. 3, pp. 39.1.1 to 39.1.4.

Primary Examiner—Douglas W. Olms

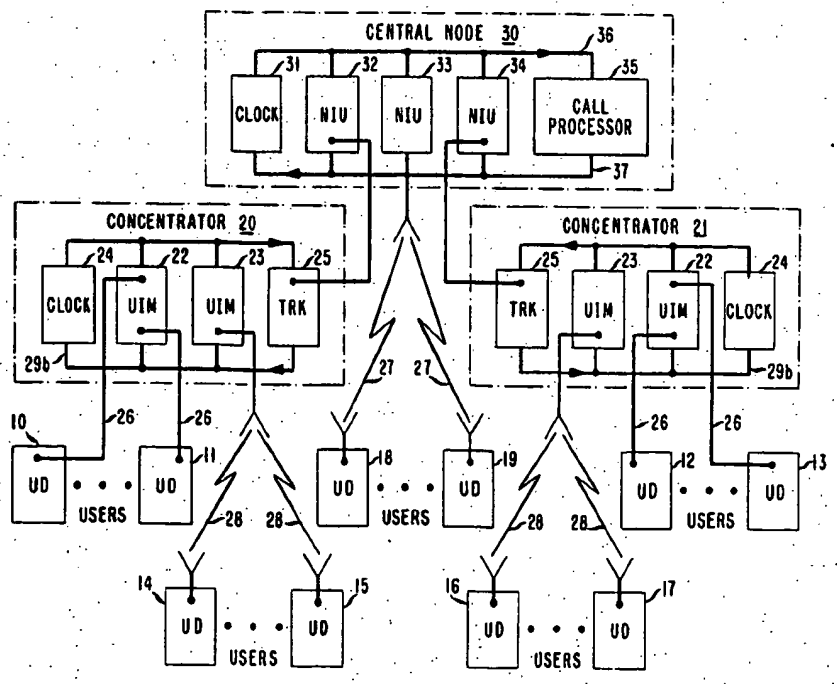
Assistant Examiner—Melvin Marcelo

Attorney, Agent, or Firm—Erwin W. Pfeifle

[57] **ABSTRACT**

The present invention relates to a wideband communication network using wireless radio transmissions either on a stand-alone basis or to supplement a hard-wired network. The exemplary network comprises (a) a plurality of transceivers associated with separate users of the network; (b) optionally at least one concentrator associated with certain separate subgroups of wireless and possibly hard-wired transceivers for providing duplex operation; and (c) a central node (i) capable of providing both duplex communications directly via a radio channel using radio links with certain subgroups of the transceivers and via a hard-wired connection with each optional concentrator, and (ii) for polling the needs of all transceivers and directing all packets of information from active transceivers through the central node and to the destined transceivers during each frame period. The network also preferably includes diversity and resource sharing techniques to provide added protection against channel impairments on an as-needed basis.

10 Claims, 2 Drawing Sheets



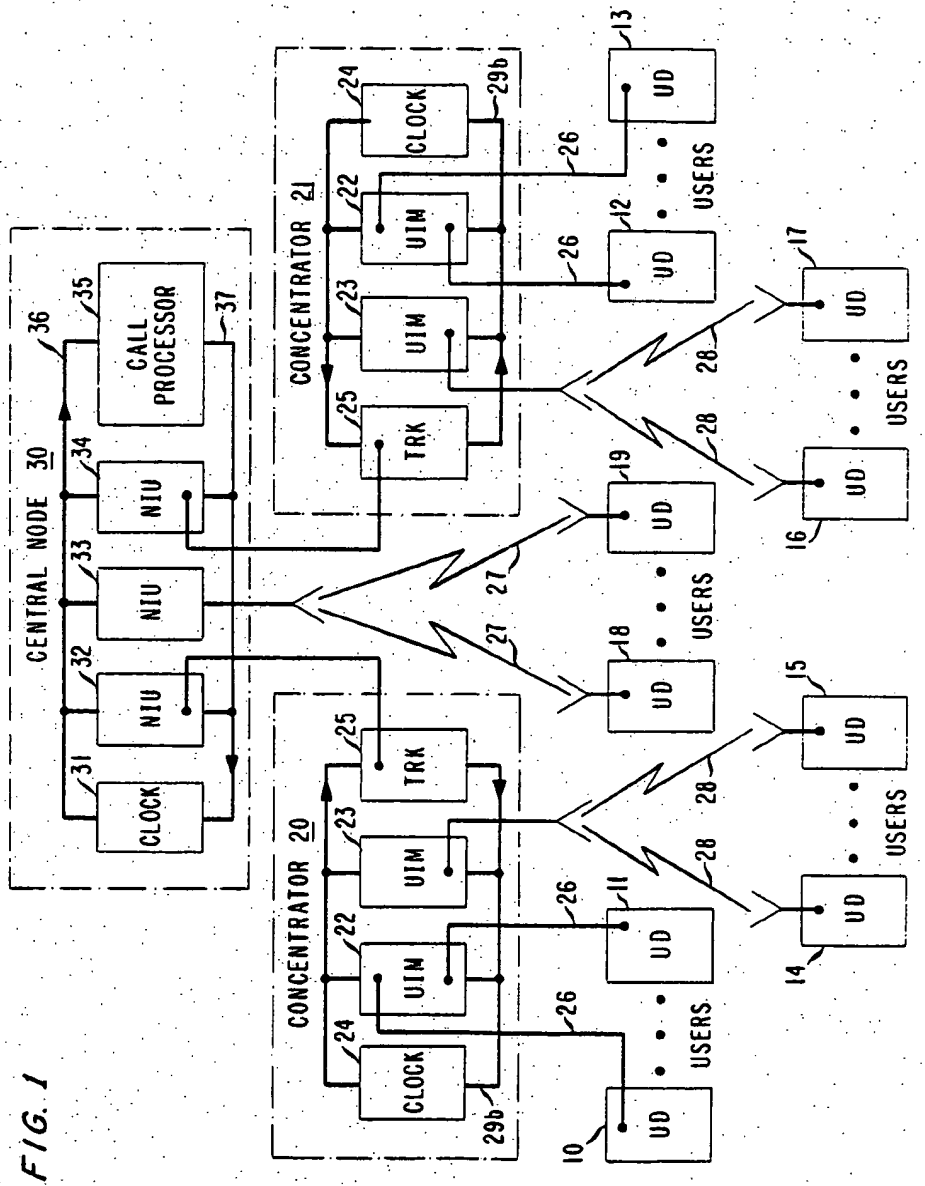
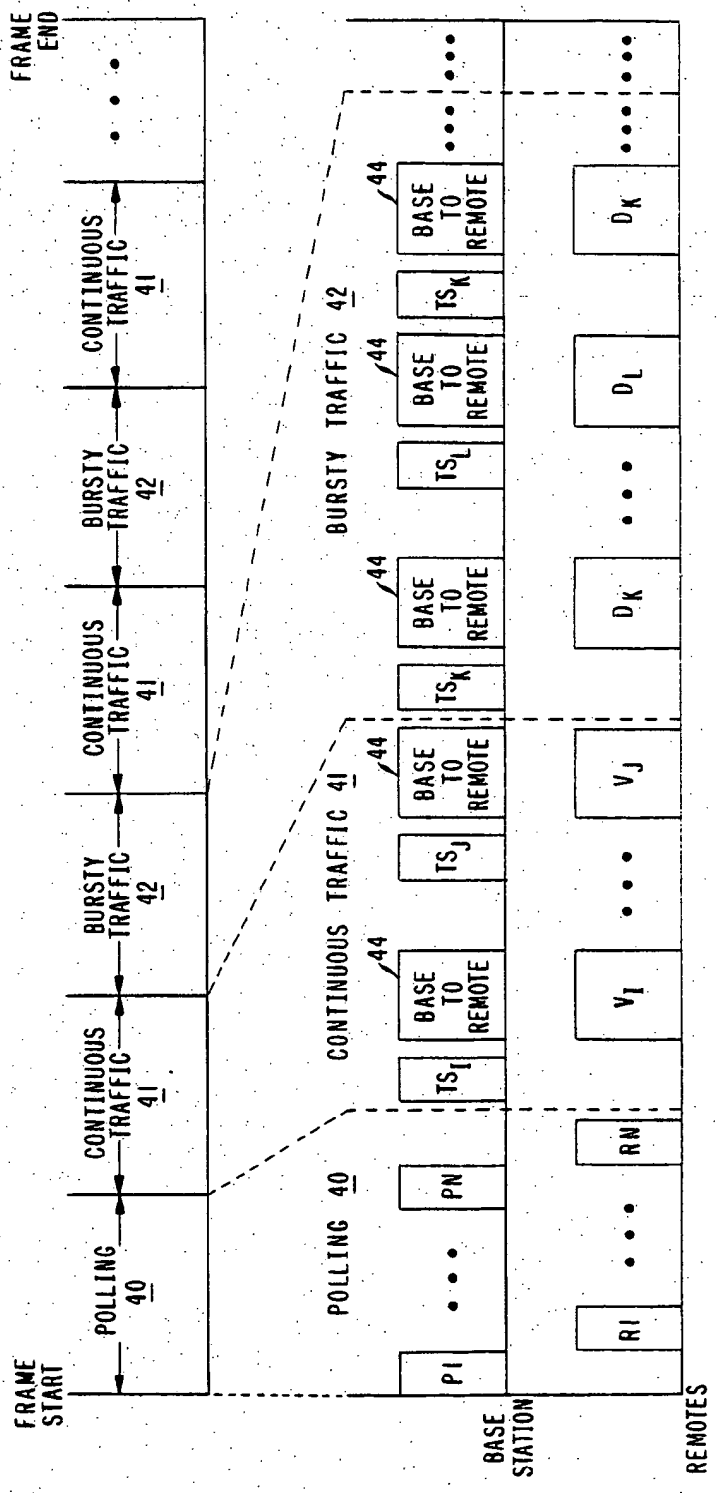

CENTRAL NODE 30
CALL PROCESSOR
NIU
NIU
NIU
CLOCK
CONCENTRATOR 21
CONCENTRATOR 20
CLOCK
UIM
UIM
TRK
UD
USERS

FIG. 1

FIG. 2


FRAME START
FRAME END
POLLING 40
CONTINUOUS TRAFFIC 41
BURSTY TRAFFIC 42
BASE TO REMOTE
44
P1
PN
RI
RN
TSI
TSJ
TSK
TSL
VI
VJ
DK
DL
BASE STATION
REMOTES

WIRELESS NETWORK FOR WIDEBAND INDOOR COMMUNICATIONS

TECHNICAL FIELD

The present invention relates to a wideband communication network using radio either on a stand-alone basis or to supplement a hard-wired network where complete portability of office design is desired.

DESCRIPTION OF THE PRIOR ART

Local Area Networks (LANs) have included many different architectures such as the bus, loop, ring, star, tree, etc. One such LAN is disclosed in the article "A New Local Area Network Architecture Using A Centralized Bus" by A. Acampora et al. in *IEEE Communications Magazine*, Vol. 22, No. 8, August 1984, at pages 12–21. There, a centralized bus is used with all user devices being hard-wired to a central node as shown in FIGS. 1–3 of the article.

Indoor wireless communications networks have also been developed over the years. In the article "Cordless Telephone System" by M. Komura et al., published in the *Japanese Telecommunications Review*, Vol. 15, No. 4, 1973, at pages 257–261, a cordless radio telephone system is disclosed which permits telephones to communicate via radio to a localized antenna which is directly connected to a base station. Another technique for wireless indoor communication is disclosed by F. Gfeller in the *IBM Technical Disclosure Bulletin*, Vol. 24, No. 8, January 1982, at pages 4043–4046 wherein an infrared microbroadcasting network for in-house data communication is disclosed. There, a host controller is directly connected to a plurality of spaced-apart transponders for transmitting 2-way communications via infrared signals with the various stations forming the in-house system.

More recently, an office information network was disclosed in *Globecom '85*, Vol. 1, Dec. 2–5, 1985, New Orleans, La. at pages 15.2.1–15.2.6 wherein a slotted-ring access protocol and a dynamic bandwidth allocation scheme offering preferential service to high-priority traffic is provided. There, a dual optical fiber ring, transmitting in opposite directions, propagates the communication signals to various nodes along the fibers. Connections between the network nodes and local facilities or servers are copper pairs or, where appropriate, wireless drops.

Indoor radio communication is not without problems, however. Buildings in general, and office buildings in particular, present a harsh environment for high-speed radio transmission because of numerous reflections from stationary objects such as walls, furniture, and movable objects such as people. The link between a given pair of transmitters and receivers is thereby corrupted by severe multipath distortion arising from the random superimposition of all reflected rays, and by shadow fading caused by the absence of line-of-sight paths. At low data rates, the effects of multipath can be characterized by Raleigh fading, while at higher rates the channel additionally exhibits dispersion over the communication band. Shadow fading is spectrally flat and characterized by a log-normal distribution.

It is to be understood that all effects vary dynamically with time as the environment slowly changes. Raleigh fading produces a wide variation in the level of signals arriving at a particular receiver from different transmitters, thereby precluding the use of standard techniques for multiple access of the radio channel. Dispersion within the channel produces serious intersymbol interference, thereby limiting the maximum data rate of the channel and causing a fraction of users to experience an unacceptably high bit error rate, and a link experiencing such condition is said to have suffered an outage and is temporarily unavailable. Therefore, the problem in the prior art is to provide a technique or network which will permit as high a data rate as possible while encountering changing conditions.

SUMMARY OF THE INVENTION

The foregoing problem in the prior art has been solved in accordance with the present invention which relates to a wireless network for wideband indoor communications using radio as the transmission medium either on a stand-alone basis or to supplement a hard-wired network. The present exemplary wideband indoor packet communications network comprises (1) a plurality of transceivers; and (2) a central node. In addition, one or more concentrators associated with certain separate groups of wireless, and possibly hard-wired, transceivers, may be present. Each transceiver is associated with a separate user of the network, and, some or all of the plurality of transceivers communicate wirelessly with associated interface units in the concentrators or central node. The central node comprises (a) means for determining and communicating the necessary transmission requireements to each of the active plurality of wireless transceivers during a first subperiod of each frame period, and (b) means for receiving packets of information from each of the plurality of transceivers, transmitted as instructed by the communicating means, and retransmitting the packets to the transceivers of the destined users during a second subperiod of the frame period. More particularly, the communicating means of the central node (i) determines the packet transmission requirements and any transmission impairments of each network user when communicating with the associated interface unit in a concentrator or central node, and (ii) causes the transceivers associated with users determined to have packet transmission requirements to transmit their packets of information with a length sufficient to overcome the determined transmission impairment,

It is also an aspect of the present invention to provide a wideband indoor communications network as described above where (1) diverstiy antennas can be used at the concentrators and central node, and one or more antennas can be used at each transceiver, and (2) access to the radio channel used by all wireless transceivers is performed by a modified polling scheme which permits resource sharing to provide added protection against channel impairments on an asneeded basis.

Other and further aspects of the present invention will become apparent during the course of the following description and by reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of an exemplary arrangement of a wideband communication network in accordance with the present invention including various hard-wired and wireless user connections; and

FIG. 2 is a diagram of a media access technique using polling that can be employed in the network of FIG. 1.

DETAILED DESCRIPTION

FIG. 1 illustrates an exemplary system topology which is functionally that of a star Local Area Network (LAN) comprising a central node 30, remote concentrators 20 and 21, and a plurality of user devices 10–19. Each user device 10–19 is associated with a separate user of the network and can communicate with central node 30 (1) via a hard-wired connection 26, as shown for the indirect connections between user devices 10–13 and concentrators 20 and 21; or (2) via a wireless link as shown for (a) the channel comprising links 27 between a subgroup of user devices 18–19 and central node 30, or (b) the indirect channel comprising links 28 between a subgroup of users 14–15 and a subgroup of users 16–17 and concentrators 20 and 21, respectively. It is to be understood that user devices 10–19 can each be coupled to a separate user terminal (not shown) such as, for example, a data device, printer, personal computer, host computer, telephone, etc.

Each of remote concentrators 20 and 21 is positioned between the associated subgroup of user terminals 10–17 and central node 30 and is shown as including (a) user interface modules (UIM) 22 and 23 which are each coupled to a separate portion of the associated subgroup of user devices 10–17 (b) a clock module 24, and (c) a trunk module 25. It is to be understood that each of exemplary concentrators 20 and 21 includes only two UIMs, for purposes of simplicity and that additional UIMs could be disposed in parallel with UIMs 22–23 shown, and connected to other portions of the associated user devices (not shown) via either separate hard-wired or wireless connections.

Each UIM 22 or 23 functions to translate the protocol of the signal received from the associated user devices to a standard protocol of the network as used by central node 30. The translated signal is then transmitted, at the appropriate time, to trunk module 25 on a time division multiplex (TDM) basis via a concentrator bus 29_a for transmission to central node 30, and vice versa for the other direction of two-way communications using concentrator bus 29_b. Where a user device already transmits and receives signals using the standard network protocol, an associated UIM need only transmit the received signal at the appropriate time based on the received clock signals from clock module 24. The trunk module 25 in each of remote concentrators 20 and 21 functions to transmit each of the signals associated with that concentrator between each of the UIMs 22 and 23 and central node 30 at the appropriate times. The clock modules 24 provide the timing signals for each of the UIMs 22 and 23, and trunk module 25 to achieve coordinated operation within the associated remote concentrator 20 or 21. Central node 30 is shown as including a clock module 31 for providing the clock signals used in central node 30; network interface units (NIU) 32-34 which are each coupled either to a separate one of remote concentrators 20 or 21 or to a separate subgroup of one or more user devices; a call processor 35; and buses 36 and 37.

To describe the operation of the present network, the network components associated only with hard-wired user devices, e.g., user devices 10–13, UIMs 22 and NIUs 32 and 34 will first be considered. Each hard-wired user device 10–13 is shown connected to the network via terminal interface wires 26 and a UIM 22. Continuous (voice) or bursty (data) traffic arriving at UIM 22 in concentrator 20 from user devices 10-11, or at UIM 22 in concentrator 21 from user devices 12–13, are formed into fixed length packets for time-multiplexed high speed transmission to central node 30 via trunk module 25. Each such packet is provided therein with a logical channel number which allows central node 30 to re-route the packet to the appropriate concentrator 20 or 21 where the indicated destination user's device is connected. Central node 30 includes a contention bus 36, 37 operating at the speed of each high speed link, to accomplish this re-routing. All traffic, including that traffic arising at a particular concentrator 20 or 21 and destined for that same concentrator, is routed through central node 30.

The receiving concentrator demultiplexes all arriving packets from central node 30 for distribution via bus 29_b to the appropriate UIM and transmission to the destined user device. Logical channel numbers are preferably assigned for the entire network at the beginning of a predetermined time period of communications by call processor 35 in central node 30. Additional device configurations and operational details are described in the article "A New Local Area Network Architecture Using A Centralized Bus" by Acampora et al. in *IEEE Communications Magazine*, Vol. 22, No. 8, August 1984, at pages 12–21.

Radio links may be introduced, as shown in FIG. 1, via either a wireless link between a UIM 23 in either one of concentrators 20 or 21 as shown for link 28, or a wireless link directly to a NIU 33 in central node 30 as shown for link 27. For link 27, the high-speed links from trunk modules 25 in concentrators 20 and 21 to central node 30 have been augmented by the inclusion of an NIU 33 in central node 30 which becomes a radio base station providing a high-speed channel to collect traffic from a subgroup of radio user devices 18–19 located throughout the building. It is to be understood that the term channel hereinafter implies full duplex operation, with separate bands used to transmit to and receive from NIU 33. This radio channel operates at a rate less than or equal to that of the central node's contention buses 36 and 37 and each of the high-speed links between trunk modules 25 and NIU's 32 and 34. With an appropriate access protocol, the radio channel may be shared among all radio users 18–19 and appear, to central node 30, as a virtual concentrator. Fixed length packets arriving over links 27 contend for the nodal bus 36 along with packets arriving via high-speed buses at NIUs 32 and 34 from trunk modules 25. The packets arriving from the wired links 26 may be rerouted by central node 30 to a radio link 27, and vice-versa, according to a destination address included in each packet.

A wireless link 28 establishes a communication path from each user of a subgroup of users, 14–15 or 16–17, to an associated UIM 23 in one of remote concentrators 20 or 21. Although multiple paths are established within a subgroup of users associated with a UIM 23 or NIU 33, these links time-share a single radio channel. More particularly, at any moment, only one radio user of a subgroup of users may access the radio channel. It should be noted that there is no need to provide an aggregate data rate over all radio links 27 or 28 in excess of the transmission speed of central node 30 since all packets must be routed through central node 30. Therefore, it is pointless to reuse the radio channel among user subgroups, as this increased capacity could not be used. Thus, by sharing a single channel, operating at the speed of central node 30, among all radio users, each

user can potentially access the full system bandwidth, and interference among clusters caused by simultaneous use of the channel by users in different clusters is avoided. From the perspective of central node 30, a radio link 28 established from each concentrator 20 or 21 to each of its subgroups of radio users appears as another wired port (UIM 22) on the concentrator.

Regarding the radio or wireless links only, each of the UIMs 23 or NIU 33 are preferably equipped with multiple antennas for diversity to protect against multipath fading, and each user device 14–19 is preferably equipped with only a single antenna, although multiple antennas could be used. The combination of limited diversity at the concentrators 20 and 21, and central node 30, along with resource sharing can be used to provide arbitrarily high availability. No direct communication is permitted among users, since all users may communicate only with concentrators 20 or 21 or central node 30. It should be understood that common media access techniques, such as Carrier Sense Multiple Access (CSMA), are inappropriate in the radio environment because free space path loss and multipath fading result in too large a variation of signal strength to insure that all channel usage can be detected. To keep the wireless user devices 14–19 inexperience, sophisticated timing requirements should be avoided. Finally, because of problems with delay spread, it is desired that the throughput of the system not be significantly reduced by a media access technique, and separate receive and transmit channels must be provided to allow full duplex operation.

For the present network shown in FIG. 1, an exemplary modified polling technique is used, with central node 30 controlling the transmit token. Polling is performed by call processor 35 in central node 30, with the radio UIMs 23, located at concentrators 20 and 21, and NIU 33, located at central node 30, being slaved to processor 35 such that, at any point in time, only one UIM 23 or NIU 33 is allowed to transmit the token to its community of UDs. It should be understood that all of radio UDs 14–19 time share a single radio channel without frequency reuse.

The present exemplary polling technique for use with the radio channel associated with the wireless UDs 14–19 is shown in FIG. 2. There, time is divided into a sequence of fixed length intervals called frames, as shown at the top of FIG. 2. At the start of each frame a polling interval 40 appears, followed by multiple intervals for transmission of continuous (voice) traffic packets 41, and bursty (data) traffic packets 42. The length of the continuous traffic intervals 41 depends on the amount of continuous traffic. This continuous traffic is transmitted periodically, at least once per frame period, with the time interval between continuous traffic intervals used for bursty traffic. Transmission of one fixed length packet per continuous traffic interval constitutes some standard grade service, e.g., 64 kbps. Continuous traffic UDs may request multiples of this basic rate by accessing multiple time slots per continuous traffic interval. The polling sequence is shown at the bottom two lines of FIG. 2 for transmissions from and to central node 30.

The following steps forming the exemplary overall transmission sequence for the radio channel are:

1. Via the UIMs 23 located at concentration 20 and 21, and NIU 33, call processor 35 at central node 30 sequentially polls each UD associated with the radio channel using sub-packets P1–PN.
2. When polled, UDs 14–19 sequentially respond, after being polled, using the associated one of packets R1–RN as to whether the UD has continuous or bursty traffic, and, if bursty traffic, the number of blocks of data.
3. Processor 35 then sequentially sends a signal, i.e., transmit token, TS_I–TS_J, to each continuous traffic user to send one fixed length packet, designated V_I to V_J, including a preset number of data symbols in each packet.
4. Processor 35 then sequentially sends a signal, designated TS_K–TS_L, i.e., a transmit token, to each bursty traffic user to send their first data block designated packets D_K–D_L, then the second data block, etc.
5. During steps 3 and 4, while the UDs are transmitting to concentrators 20 and 21 in blocks V_I–V_J and D_K–D_L, processor 35, through the UIMs 23 at the concentrators, is transmitting voice and data to the UDs 14–17 in associated blocks 44.
6. When it is time again for continuous traffic to be transmitted, then step 3 is reiterated.
7. When it is time again for polling, i.e., the beginning of another frame, then step 1 is reiterated.

The above described polling technique meets necessary requirements since (a) the system handles continuous traffic, i.e., periodic data or voice, with priority, (b) the system has the same maximum data rate for each use, i.e., a fair distribution of resources, which depends on the system loading, (c) there is no timing requirements at the remote UDs 14–19, (d) the throughput on the channel is not significantly reduced by this technique because the polling has a low duty cycle, mainly due to the short propagation delays between the concentrators 20, 21 and the remote UDs 14–19, and (e) the system has duplex operation.

What must also be considered is that in a multipath environment, paths of different lengths cause delay spread at a receiver. The delay spread, i.e., the dispersion or frequency selective fading in the channel, produces intersymbol interference which limits the maximum data rate in a given building and depends primarily on the rms delay spread and not the delay spread function. Thus, within the coverage area, there is some probability that the received signal bit error rate (BER) for each UD is more than the required value, hereinafter called the outage probability. If one UD 14–19 does not work in one location, the user can move the UD or its antenna. However, the delay spread may vary slowly with time as people and objects move within the building. Therefore, it is desirable to keep the outage probability due to delay spread as low as possible so that the wireless system is almost as reliable as any wired portion of the system.

In addition to the technique described above, resource sharing can be used to increase the maximum data rate and/or decrease the outage probability. With resource sharing, users normally transmit at some high rate R_1. When channel conditions between concentrators 20 or 21, or central node 30, and a particular UD no longer permits operation at this high rate., the rate is lowered to some value such as R_2 such that the BER objective is maintained. Such techniques are well known in the satellite system art as disclosed, for example, in the articles by A. S. Acampora in *BSTJ*, Vol. 58, No. 9, November 1979, at pages 2097–2111; and *IEEE Journal On Selected Areas In Communications*, Vol. SAC-1, Jan. 1983, at pages 133–142 where a pool of spare time slots are used, and each packet is transmitted

with or without coding, to reduce the outage probability. Although it takes longer to complete transmission at this lower rate, the number of users simultaneously slowed down is usually a small fraction of the total population, and the overall throughput remains high. More particularly, during non-fade conditions, convolutional codes with a large channel signaling alphabet are employed to permit a high rate of information transfer as described hereinbefore for the 7-step transmission sequence, and when the fade depth exceeds the built in fade margin, the signaling alphabet is reduced and enough time slots are borrowed from a resource sharing reserved time slot pool to maintain the data rate at the fade site. From the prior art, it is known that a small pool of spare time slots can protect a large community of users. In the present technique, the use of coding during fade events is not considered because the channel is dispersive.

Implementation of resouce sharing with two transmission rates requires modification of the 7-step media access technique described hereinbefore. With resource sharing, transmission would normally be at the higher rate R_1 during non-transmission impairment periods. If errors are detected at the higher rate via standard error detection techniques, a receiver in UDs **14–19**, UIMs **23**, or NIU **33** can request call processor **35** to schedule a retransmission of the last block of data at the lower rate R_2. Call processor **35** would then cause the transmitter to retransmit the last block of information during a subsequent corresponding continuous **41** or bursty **42** traffic period at the lower data using, for example, a longer block V_i, D_i, or **44**, or two or more equal length blocks. A transmitter for accomplishing such technique of resource sharing is described, for example, in U.S. Pat. No. 4,309,764 issued to A. Acampora on Jan. 5, 1982, and the previously cited article to A. Acampora in *BSTJ*, Vol. 58, No. 9, November 1979, at pages 2097–2111. Periodically the transmitter can retry transmission at the higher rate. The frequency of retries depends on the dynamics of the delay spread in the channel. Requests for lower rate transmission and retries at the higher rate need only occur infrequently since the channel normally varies very slowly with time.

What is claimed is:

1. A wideband packet communication network comprising:

a plurality of transmitters (**10–19**), each transmitter being associated with a separate user or group of users of the network for transmitting packets of information between an active user or group of users and the network via either one of a hard-wired or wireless connection during a frame period; and

a central node (**30**) for communicating with each of the plurality of transmitters via the hard-wired or wireless connection, the central node comprising,

processor means (**35**) for (a) determining packet transmission requirements associated with each transmitter communicating with the central node via a wireless connection during a first subperiod of each frame period, (b) causing each wireless transmitter determined to have a packet transmission requirement, to transmit its packets of information during a separate second subperiod of time of each frame period, (c) detecting during the first and/or second subperiods of each frame period, transmission impairments associated with each wireless transmitter, and (d) causing packets of information transmitted from each transmitter determined to have a transmission impairment to be transmitted at a transmission rate sufficient to lessen the determined transmission impairment, and

means (**32–34**) for (a) receiving packets of information from the plurality of transmitters of the network, and (b) retransmitting the packets to receivers associated with the destined users of the packets of information via an appropriate hard-wired or wireless connection.

2. A wideband packet communication network according to claim **1** wherein the receiving and retransmitting means comprises:

a high-speed bus for propagating packets of information from the plurality of transmitters on a time division multiplexed basis; and

a plurality of network interface units (NIUs), each NIU being associated with a separate subgroup of one or more of the plurality of transmitters, and connected to the tramsitters of the separate subgroup via a wireless communication link or separate hard-wired connections for receiving the packets of information from the associated subgroup of transmitters and transmitting each packet over the high-speed bus during a free time slot period to the NIU associated with a user destined to receive the packet of information.

3. A wideband packet communication network according to claim **2** wherein the network further comprises:

at least one concentrator, each concentrator being disposed between a separate subgroup of the plurality of transmitters and a predetermined one of the plurality of NIUs, each concentrator comprising:

a plurality of user interface modules (UIM), each UIM providing duplex communications with a separate portion of the subgroup of transmitters associated with the concentrator, where at least one of the subgroup portions communicates with its UIM via a separate wireless link,

a trunk module for providing duplex communications between the UIMs of the concentrator and the predetermined associated one of the plurality of NIUs in the central node on a time division multiplexed basis, and

a bus for propagating packets of information between the plurality of UIMs of the concentrator and the trunk module on a time division multiplexed basis.

4. A wideband packet communication network according to claim **1**, **2** or **3** wherein the processor means comprises:

means responsive to the beginning of a frame period for (a) sequentially sending first control signals (P_i) to each of the plurality of transmitters and sequentially receiving second control signals (R_i) from the transmitters indicative of whether or not a transmitter has a packet of information to be transmitted during the frame period, and (b) in response to each received second control signal indicating that a transmitter is active and has a packet of information to be sent, sequentially transmitting third control signals (TS_i) to the active transmitters for causing the packet of information to be sent by the transmitter for routing by the central node to a destined user of the packet of information.

5. A wideband packet communication network according to claim 4 wherein

the receiving and retransmitting means in the central node comprises means for detecting that a packet of information was received from a transmitter with a bit error rate that is less than a predetermined value, and for generating a separate transmission impairment control signal to the determining and causing means; and

the determining and causing means is responsive to a transmission impairment control signal from the receiving and retransmitting means for transmitting a subsequent second control signal to the transmitter detected as having a transmission impairment for causing the transmitter to retransmit the packet of information at a slower data rate using a predetermined resource sharing technique.

6. A wideband packet communication network according to claim 5 wherein

the receiving and retransmitting means includes diversity antennas associated with wireless connections.

7. A wideband packet communication network according to claim 1,2 or 3 wherein

the receiving and retransmitting means includes diversity antennas associated with the wireless connections.

8. A method of transmitting information between a plurality of transmitters and a central node, including a processor means, via either one of a hard-wired or wireless connection during a frame period in a wideband packet communication network, each transmitter being associated with a separate user or group of users of the network, the method comprising the steps of:

(a) the processor means in the central node determining the packet transmission requirements of each transmitter communicating with the central node during a first subperiod of time of each frame period;

(b) causing a wireless transmitter determined in step (a) to have packet transmission requirements, to transmit its packets of information during a separate second subperiod of time of each frame period;

(c) the processor means detecting, during the first and/or second subperiods of time of each frame period, transmission impairments associated with each wireless transmitter; and

(d) the processor means causing packets of information transmitted from each transmitter determined to have a transmission impairment in step (c) to be transmitted at a transmission rate sufficient to lessen the determined transmission impairment.

9. A method according to claim 8 wherein the method comprises the further steps of:

in performing step (a) performing the substeps of

(a1) the processor means sequentially transmitting first control signals (P_i) to each of the plurality of transmitters, and

(a2) sequentially receiving second control signals (R_i) from the plurality of transmitters indicative of whether or not a transmitter has a packet of information to be transmitted during the frame period; and

in performing step (b), performing the step of

(b1) in response to each received second control signal in step (a2) indicating that a transmitter is active and has a packet of information to be sent, sequentially transmitting third control signals (TS_i) to the active transmitters for causing the packet of information to be sent by the transmitter for routing by the central node to a destined user of the packet of information.

10. A method according to claim 8 or 9 wherein in performing step (c) performing the substeps of:

(c1) detecting at the central node that a packet of information was received from a transmitter with a bit error rate that is less than a predetermined value;

(c2) transmitting a subsequent second control signal to the transmitter detected as having a transmission impairment in response to the detection of a bit error rate more than a predetermined value in step (c1); and

(c3) a transmitter having a transmission impairment being responsive to a subsequent second control signal transmitted in step (c2) for retransmitting the packet of information at a slower transmission rate using a predetermined resource sharing technique such that the packet of information is received at the central node with a bit error rate below the predetermined value.

* * * * *

US006366957B1

(12) **United States Patent**
Na

(10) **Patent No.: US 6,366,957 B1**
(45) **Date of Patent: Apr. 2, 2002**

(54) **COMPUTER SYSTEM HAVING REMOTE WAKE-UP FUNCTION AND REMOTE WAKE-UP METHOD THEREOF**

(75) Inventor: **Seung-Ju Na**, Seoul (KR)

(73) Assignee: **Samsung Electronics Co., Ltd.**, Suwon (KR)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/262,739**

(22) Filed: **Mar. 5, 1999**

(30) **Foreign Application Priority Data**

Mar. 5, 1998 (KR) 98-7318

(51) **Int. Cl.**[7] **G06F 15/16**; G06F 11/30

(52) **U.S. Cl.** **709/229**; 713/202

(58) **Field of Search** 709/229, 217, 709/222, 225; 713/2, 202, 180

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,421,009	A		5/1995	Platt
5,577,209	A		11/1996	Boyle et al.
5,802,305	A		9/1998	McKaughan et al.
5,826,015	A		10/1998	Schmidt
5,828,833	A		10/1998	Belville et al.
5,864,683	A		1/1999	Boebert et al.
5,974,547	A	*	10/1999	Klimento 713/2
6,101,608	A	*	8/2000	Schmidt et al. 713/202
6,119,228	A	*	9/2000	Agelo et al. 713/180

* cited by examiner

Primary Examiner—Glenton B. Burgess
Assistant Examiner—Kenneth W. Fields
(74) *Attorney, Agent, or Firm*—Robert E. Bushnell, Esq.

(57) **ABSTRACT**

A computer system having a remote wake-up function capable of storing confidential information, and a remote wake-up method thereof. The computer system having a remote wake-up function includes: a network information storage portion for storing network information including a network address and a password; and a magic packet controller for receiving a magic packet via a physical layer portion, comparing a network address and a password which are contained in a magic packet, with the network address and the password stored in the network information storage portion, and generating a wake-up control signal to transfer to a power management unit of the computer system only when the compared network addresses and passwords are the same each other, wherein the computer system suspended is booted by the wake-up control signal. Therefore, when waking up remotely the computer system via a network, it is determined whether or not such remote waking up is by an authorized supervisor system. As a result, the computer system can be prevented from having information stolen therefrom by a user with bad intentions. Also, as a further result, the computer system can avoid becoming damaged by a user with bad intentions.

21 Claims, 7 Drawing Sheets

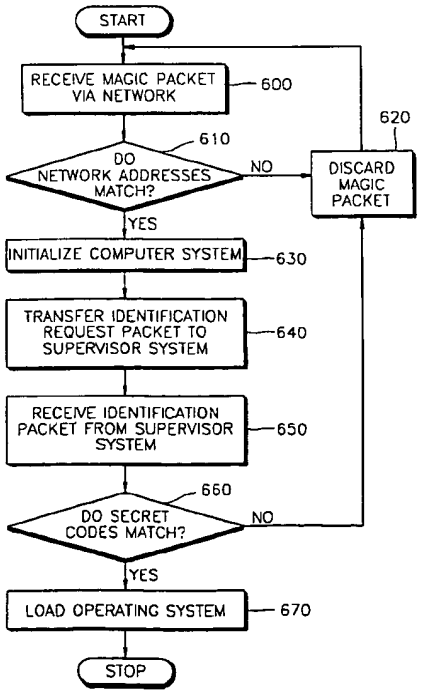


FIG. 1

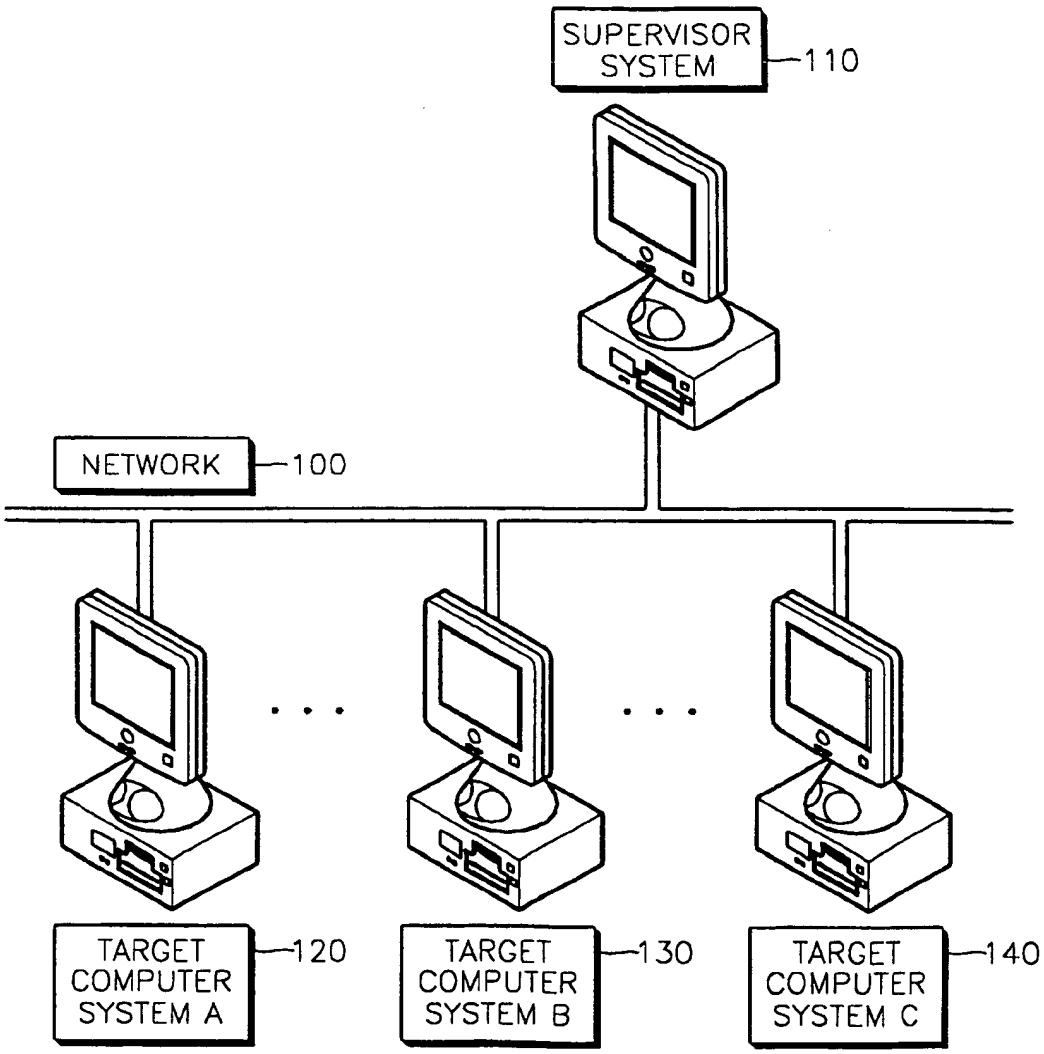

SUPERVISOR SYSTEM
110
NETWORK
100
TARGET COMPUTER SYSTEM A
120
TARGET COMPUTER SYSTEM B
130
TARGET COMPUTER SYSTEM C
140

FIG. 2

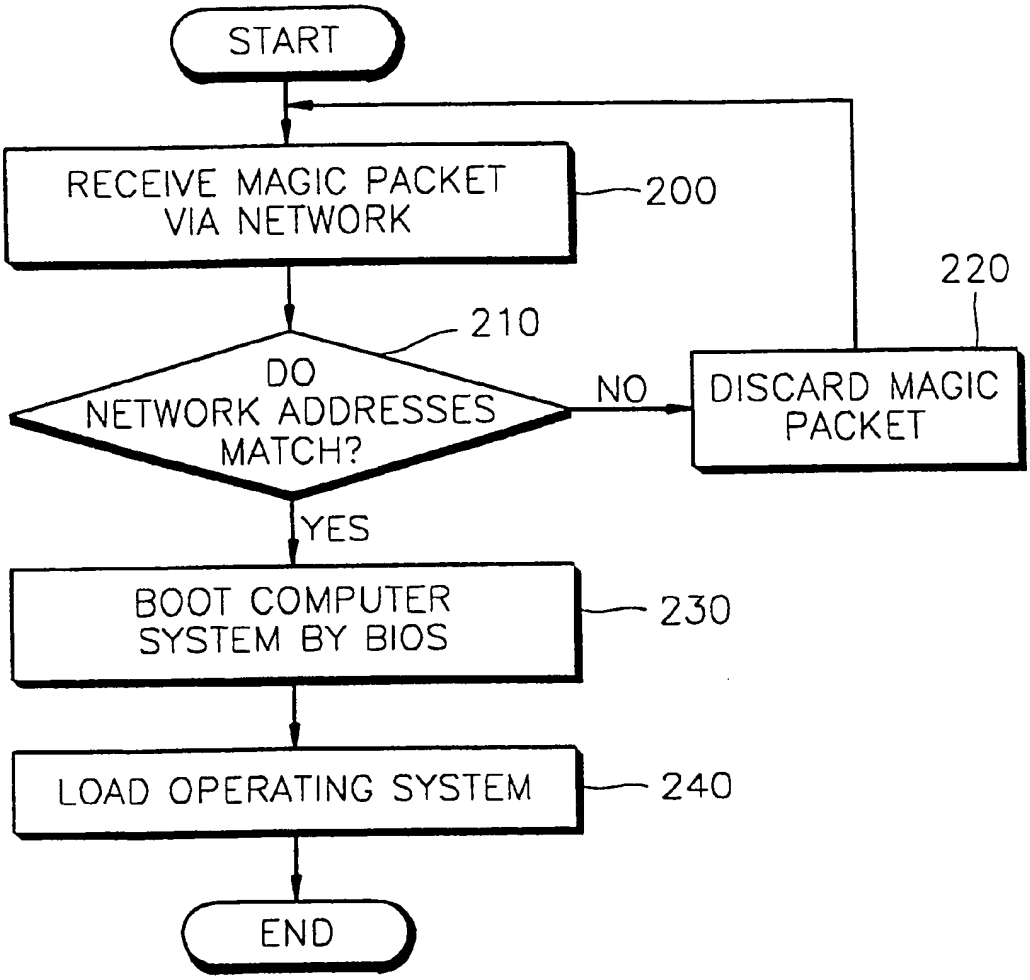

START
RECEIVE MAGIC PACKET VIA NETWORK
200
210
DO NETWORK ADDRESSES MATCH?
NO
220
DISCARD MAGIC PACKET
YES
BOOT COMPUTER SYSTEM BY BIOS
230
LOAD OPERATING SYSTEM
240
END

FIG. 3

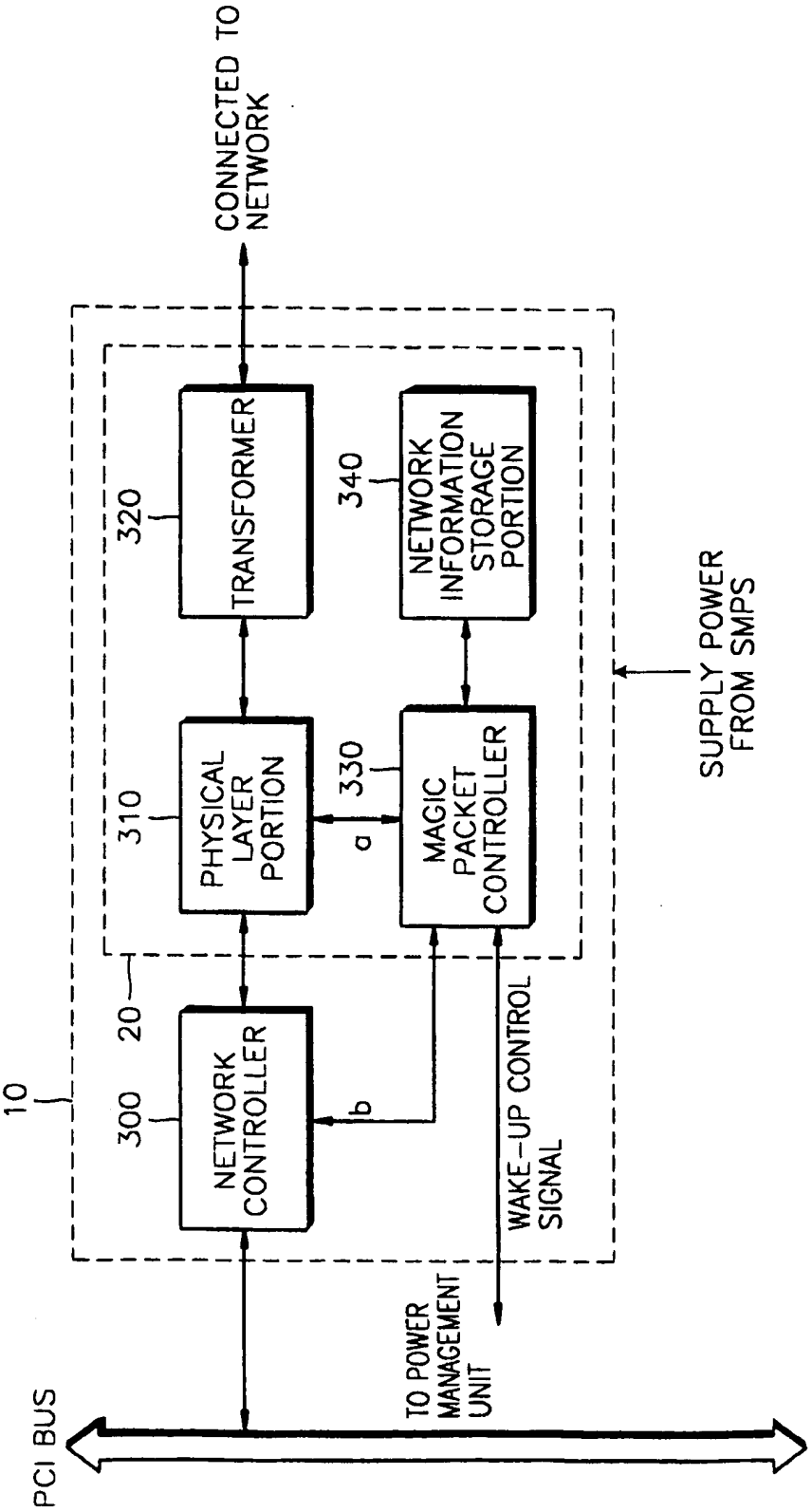

CONNECTED TO NETWORK
TRANSFORMER
320
NETWORK INFORMATION STORAGE PORTION
340
SUPPLY POWER FROM SMPS
PHYSICAL LAYER PORTION
310
330
a
MAGIC PACKET CONTROLLER
20
10
300
NETWORK CONTROLLER
b
WAKE-UP CONTROL SIGNAL
TO POWER MANAGEMENT UNIT
PCI BUS

FIG. 4

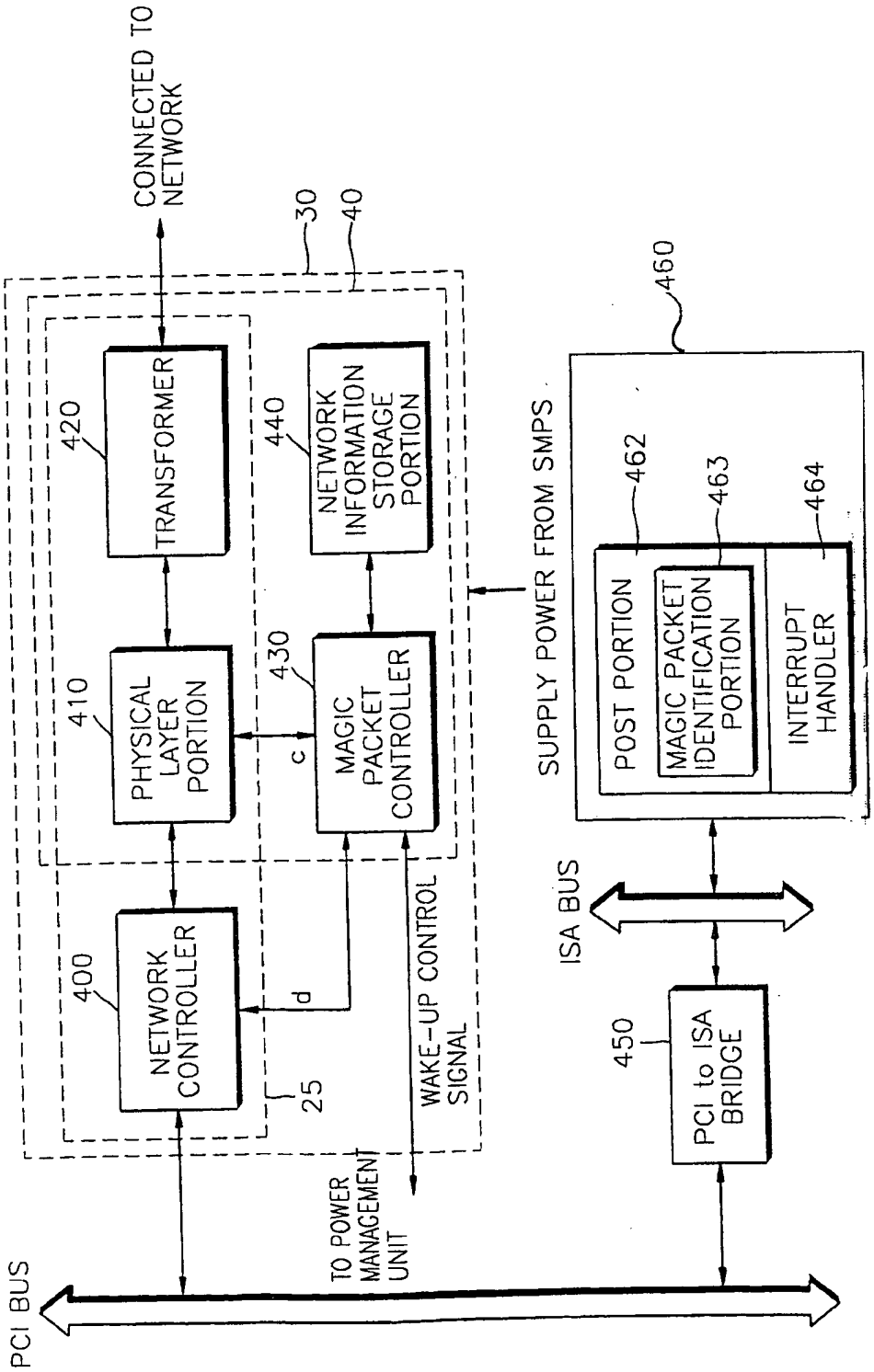

CONNECTED TO NETWORK
30
40
460
420
TRANSFORMER
440
NETWORK INFORMATION STORAGE PORTION
462
463
464
SUPPLY POWER FROM SMPS
POST PORTION
MAGIC PACKET IDENTIFICATION PORTION
INTERRUPT HANDLER
410
PHYSICAL LAYER PORTION
430
c
MAGIC PACKET CONTROLLER
ISA BUS
400
NETWORK CONTROLLER
d
25
WAKE-UP CONTROL SIGNAL
450
PCI to ISA BRIDGE
TO POWER MANAGEMENT UNIT
PCI BUS

FIG. 5

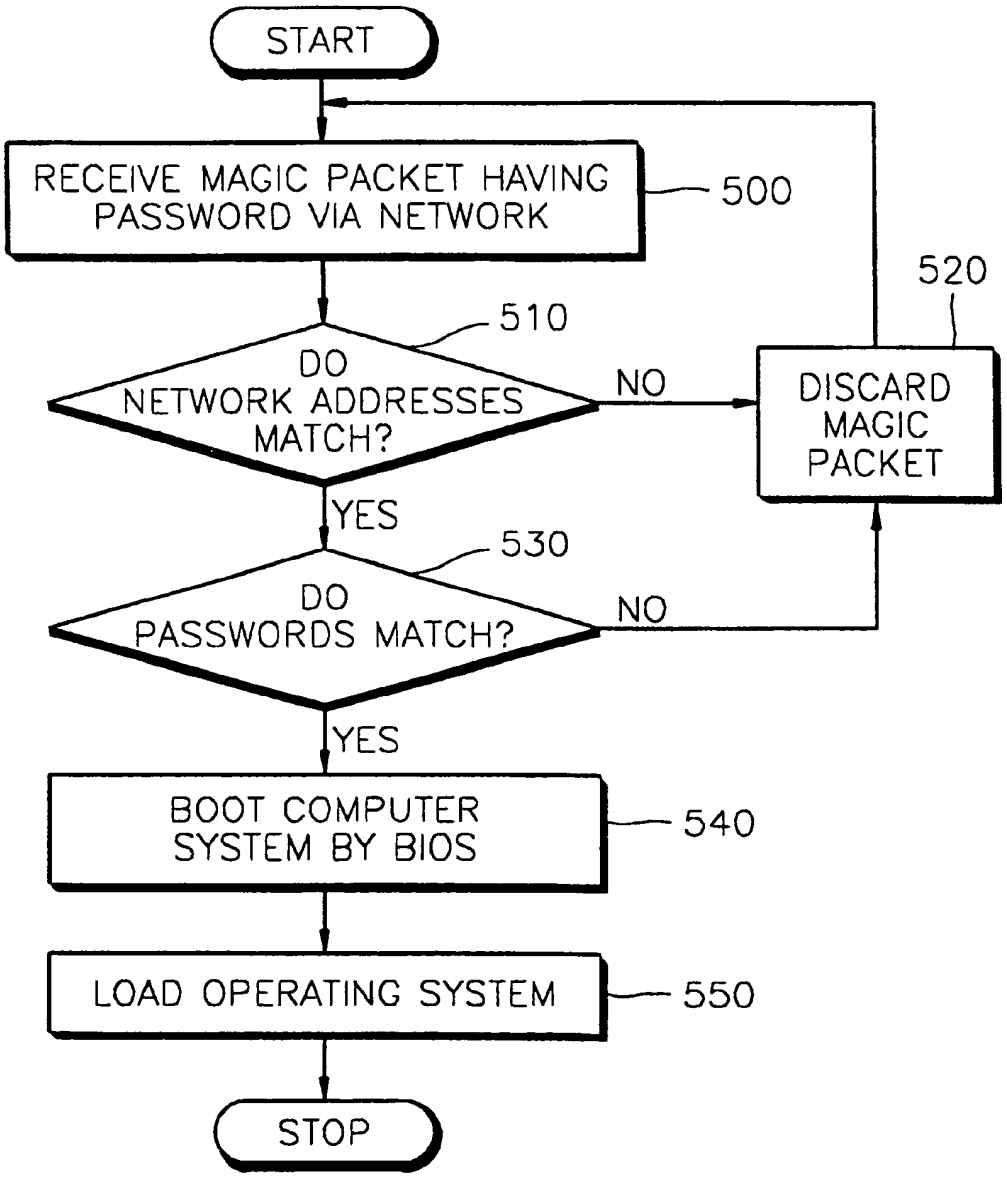

START
RECEIVE MAGIC PACKET HAVING PASSWORD VIA NETWORK
500
DO NETWORK ADDRESSES MATCH?
510
NO
DISCARD MAGIC PACKET
520
YES
DO PASSWORDS MATCH?
530
NO
YES
BOOT COMPUTER SYSTEM BY BIOS
540
LOAD OPERATING SYSTEM
550
STOP

FIG. 6

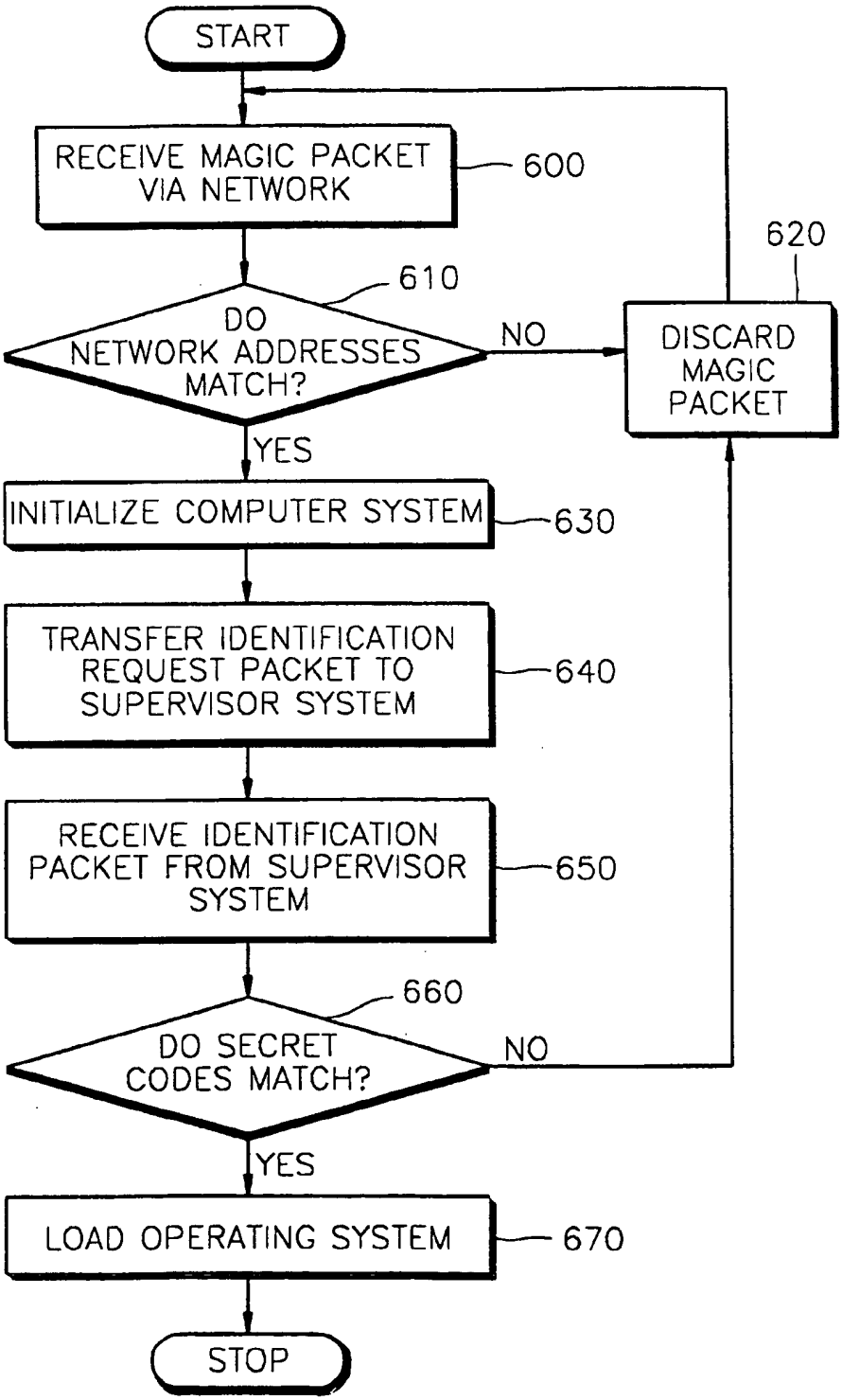
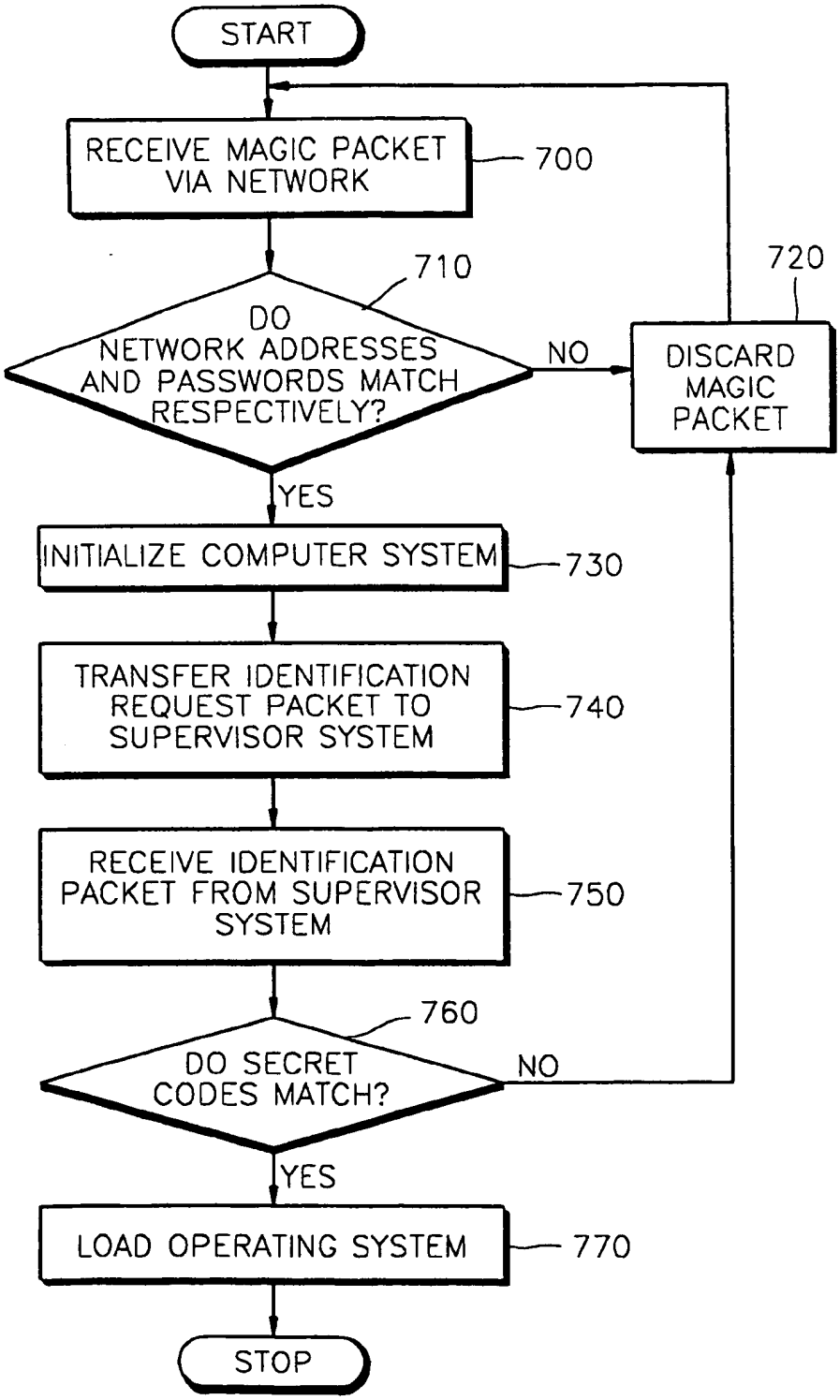

START
RECEIVE MAGIC PACKET VIA NETWORK
600
620
610
DO NETWORK ADDRESSES MATCH?
NO
DISCARD MAGIC PACKET
YES
INITIALIZE COMPUTER SYSTEM
630
TRANSFER IDENTIFICATION REQUEST PACKET TO SUPERVISOR SYSTEM
640
RECEIVE IDENTIFICATION PACKET FROM SUPERVISOR SYSTEM
650
660
DO SECRET CODES MATCH?
NO
YES
LOAD OPERATING SYSTEM
670
STOP

FIG. 7


START
RECEIVE MAGIC PACKET VIA NETWORK
700
710
DO NETWORK ADDRESSES AND PASSWORDS MATCH RESPECTIVELY?
NO
720
DISCARD MAGIC PACKET
YES
INITIALIZE COMPUTER SYSTEM
730
TRANSFER IDENTIFICATION REQUEST PACKET TO SUPERVISOR SYSTEM
740
RECEIVE IDENTIFICATION PACKET FROM SUPERVISOR SYSTEM
750
760
DO SECRET CODES MATCH?
NO
YES
LOAD OPERATING SYSTEM
770
STOP

COMPUTER SYSTEM HAVING REMOTE WAKE-UP FUNCTION AND REMOTE WAKE-UP METHOD THEREOF

CLAIM OF PRIORITY

This application makes reference to, incorporates the same herein, and claims all benefits accruing under 35 U.S.C. § 119 from an application entitled COMPUTER SYSTEM HAVING THE FUNCTION OF EMOTE WAKING UP AND METHOD FOR REMOTE WANG UP THE COMPUTER SYSTEM earlier filed in the Korean Industrial Property Office on the 5th day of March 1998, and there duly assigned Ser. No. 98-7318, a copy of which is annexed hereto.

BACKGROUND OF THE INVENTION

1. Technical Field

The present invention relates to a computer system, and more particularly to a computer system having a remote wake-up function and to a remote wake-up method of the computer system.

2. Related Art

Computer systems are information handling systems that are utilized by many individuals and businesses today. A computer system can be defined as a microcomputer that includes a central processing unit (CPU), a volatile memory, a non-volatile memory such as read only memory (ROM), a display monitor, a keyboard, a mouse or other input device such as a trackball, a floppy diskette s drive, a compact disc-read only memory (CD-ROM) drive, a modem, a hard disk storage device, and a printer. A computer system's main board, which is a printed circuit board known as a motherboard, is used to electrically connect these components together. A computer system can be a desktop computer, a portable computer such as a notebook computer or palm-sized computer, or other type of computer.

The central processing unit is often described as a microprocessor. The microprocessor is an electronic component having internal logic circuitry handling most, if not all, the data processing in the computer system. The internal logic circuitry of microprocessors is typically divided into three functional parts known as the input/output (I/O) unit, the control unit, and the arithmetic-logic unit (ALU). These three functional parts interact together and determine the power and performance of the microprocessor. The combination of the control unit and the arithmetic-logic unit can be referred to as the central processing unit. Also, the combination of the input/output unit, the control unit, and the arithmetic-logic unit can be referred to as the central processing unit.

One example of non-volatile memory is read only memory (ROM). Information stored in non-volatile memory can remain unchanged even when there is a power failure. The information stored in non-volatile memory will stay there until it is changed. Read only memory is used to store important information such as instructions for the central processing unit. There are different types s of read only memory including electrically-erasable-programmable-read-only-memory (EEPROM) chip and flash-read-only-memory (flash-ROM). The flash-ROM can also be referred to as flash memory.

Computer systems include a basic input output system (BIOS) which is an especially important program stored in read only memory. The basic input output system tests a computer every time the computer is powered on. The basic input output system can allocate a computer system's resources automatically, making adjustments needed to accommodate new hardware. Also, the basic input output system governs how system board components interact.

When the computer system is powered on, the basic input output system immediately takes control of the computer system and its components. The first duty of the basic input output system is to perform a series of diagnostic routines called the power on self test (POST) routine, which ensures that every part of the computer system's hardware is functioning properly. An operating system is a group of functions that are used for operating the computer system after the power on self test routine is performed. Microsoft Windows 98 is one example of an operating system.

A plurality of computer systems can be connected by a network. One or more of the plurality of computer systems connected by the network can be a supervisory computer system. Each one of the computer systems can include software programs. An operator can use the supervisory computer system to update the software programs of the other computer systems connected to the network. The update performed by the operator can be performed using the network itself.

I have discovered that a user with bad intentions may utilize a computer network to read confidential information stored in another computer connected to the network and also damage another computer system connected to the network. Efforts have been made to improve computers interconnected on networks and to improve the networks themselves.

Exemplars of recent efforts in the art include U.S. Pat. No. 5,864,683 for SYSTEM FOR PROVIDING SECURE INTERNETWORK BY CONNECTING TYPE ENFORCING SECURE COMPUTERS TO EXTERNAL NETWORK FOR LIMITING ACCESS TO DATA BASED ON USER AND PROCESS ACCESS RIGHTS issued to Boebert et al., U.S. Pat. No. 5,828,833 for METHOD AND SYSTEM FOR ALLOWING REMOTE PROCEDURE CALLS THROUGH A NETWORK FIREWALL issued to Belville et al., U.S. Pat. No. 5,826,015 for METHOD AND APPARATUS FOR SECURE REMOTE PROGRAMMING OF FIRMWARE AND CONFIGURATIONS OF FIRMWARE AND CONFIGURATIONS OF A COMPUTER OVER A NETWORK issued to Schmidt, U.S. Pat. No. 5,802,305 for SYSTEM FOR REMOTELY WAKING A SLEEPING COMPUTER IN POWER DOWN STATE BY COMPARING INCOMING PACKET TO THE LIST OF PACKETS STORING ON NETWORK INTERFACE CARK issued to McKaughan et al., U.S. Pat. No. 5,5777,209 for APPARATUS AND METHOD FOR PROVIDING MULTI-LEVEL SECURITY FOR COMMUNICATION AMONG COMPUTERS AND TERMINALS ON A NETWORK issued to Boyle et al., and U.S. Pat. No. 5,421,009 for METHOD OF REMOTELY INSTALLING SOFTWARE DIRECTLY FROM A CENTRAL COMPUTER issued to Platt.

While these recent efforts provide advantages, I note that they fail to adequately provide a computer system having remote wake-up function and remote wake-up method thereof.

SUMMARY OF THE INVENTION

To solve the above problems, objectives of the present invention are to provide a computer system having a remote wake-up function, which is awoken only by a magic packet transmitted by an authorized supervisor system, and to provide a remote wake-up method thereof.

According to an aspect of the objectives of the present invention, there is provided a computer system connected to a network having a remote wake-up function, comprising a network connection portion including a transformer, a physical layer portion and a network controller, wherein the network connection portion further comprises: a network information storage portion for storing network information including a network address and a password; and a magic packet controller for receiving a magic packet via the physical layer portion, comparing a network address and a password which are contained in the magic packet, with the network address and the password stored in the network information storage portion, and generating a wake-up control signal to transfer to a power management unit of the computer system only when the compared network addresses and passwords are the same each other, and the computer system suspended is booted by the wake-up control signal.

According to another aspect of the objective of the present invention, there is provided a method for remotely waking up a computer system connected to a network, comprising the steps of: (a) receiving a magic packet via the network; (b) identifying a network address contained in the magic packet; (c) identifying a password contained in the magic packet; (d) generating a wake-up control signal; and (e) booting the computer system by a basic input/output system (BIOS), wherein the waking-up on the computer system stops when the network address and the password are not identified in the steps (b) and (c).

Also, there is provided a method for remotely waking up a computer system connected to a network, comprising the steps of: (a) receiving a magic packet via a network; (b) identifying a network address contained in the magic packet; (c) performing a power on self test (POST) by a basic input/output system (BIOS); (d) transferring an identification request packet to a supervisor system identified based on the network address contained in the magic packet; (e) receiving an identification packet from the supervisor system; (f) identifying the identification packet; and (g) loading an operating system for operating the computer system, wherein the waking-up on the computer system stops when the network address and the identification packet are not identified in the steps (b) and (f).

To achieve these and other objects in accordance with the principles of the present invention, as embodied and broadly described, the present invention provides an apparatus, comprising: a computer system processing first data when said computer system is in a first mode corresponding to a full power mode, said computer system not processing the first data when said computer system is in a second mode not corresponding to said full power mode; a storage unit storing a first address and a first password; and a control unit being coupled to said storage unit and said computer system, said control unit receiving a packet signal including a second address and a second password, comparing said first address and said first password with said second address and said second password respectively, and generating a control signal when said first address corresponds to said second address and said first password corresponds to said second password, said computer system being booted and converted to said first mode from said second mode in response to said control signal.

To achieve these and other objects in accordance with the principles of the present invention, as embodied and broadly described, the present invention provides a method, comprising: receiving a packet signal via a network unit, said network unit being coupled to a first computer system and a second computer system; determining whether a first network address contained in said packet signal corresponds to a predetermined address; determining whether a first password contained in said packet signal corresponds to a predetermined password; generating a control signal when said first network address and said first password correspond to said predetermined address and said predetermined password respectively; and booting said first computer system by a basic input output system in response to said control signal.

To achieve these and other objects in accordance with the principles of the present invention, as embodied and broadly described, the present invention provides a method, comprising: receiving a packet signal via a network unit, said network unit being coupled to at least a first computer system; detecting whether a first network address contained in said packet signal corresponds to a predetermined address; when said first network address corresponds to said predetermined address, performing a power on self test on said first computer system by a basic input output system; transmitting an identification request signal to a second computer system, said second computer system corresponding to said first network address contained in said packet signal; receiving an identification packet signal from said second computer system in response to said identification request signal; determining whether said identification packet signal corresponds to a predetermined identification code; and when said identification packet signal corresponds to said predetermined identification code, loading an operating system for operating said first computer system.

The present invention is more specifically described in the following paragraphs by reference to the drawings attached only by way of example. Other advantages and features will become apparent from the following description and from the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

In the accompanying drawings, which are incorporated in and constitute a part of this specification, embodiments of the invention are illustrated, which, together with a general description of the invention given above, and the detailed description given below, serve to exemplify the principles of this invention.

FIG. **1** is a diagram showing the structure of computer systems connected via a network;

FIG. **2** is a flowchart illustrating a remote wake-up method for a computer system;

FIG. **3** is a block diagram showing the structure of a network connection portion of a computer system corresponding to a first preferred embodiment, in accordance with the principles of the present invention;

FIG. **4** is a block diagram showing the structures of a network connection portion and a basic input/output system (BIOS) of a computer system corresponding to a second preferred embodiment, in accordance with the principles of the present invention;

FIG. **5** is a flowchart illustrating a remote wake-up method of the computer system shown in FIG. **3**, through identification of a password, corresponding to a preferred embodiment, in accordance with the principles of the present invention;

FIG. **6** is a flowchart illustrating a remote wake-up method of the computer system shown in FIG. **4**, through identification of a packet, corresponding to another preferred embodiment, in accordance with the principles of the present invention; and

FIG. **7** is a flowchart illustrating a remote wake-up method of the computer system shown in FIG. **4**, through identification of a password and a packet, corresponding to still another preferred embodiment, in accordance with the principles of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

While the present invention will be described more fully hereinafter with reference to the accompanying drawings, in which a preferred embodiment of the present invention is shown, it is to be understood at the outset of the description which follows that persons of skill in the appropriate arts may modify the invention here described while still achieving the favorable results of this invention. Accordingly, the description which follows is to be understood as being abroad, teaching disclosure directed to persons of skill in the appropriate arts, and not as limiting upon the present invention.

Turn now to FIG. **1**, which shows the structure of computer systems connected via a network. FIG. **1** shows a plurality of computer systems **110**, **120**, **130**, **140** connected by a network **100**. In general, when the computer systems connected to the network **100** are not in use, each computer system is suspended by a power management unit installed therein. Also, a supervisor system **110** has a need to access the computer systems connected to the network **100** in order to manage the entire computer system, or upgrade, maintain, or repair software installed in the entire computer system. First of all, the supervisor system **110** must wake up target computer systems **120**, **130** and **140** which are in suspension.

Turn now to FIG. **2**, which shows a flowchart illustrating a remote wake-up method for a computer system. A method for waking up suspended computer systems by a remote supervisor system is illustrated in FIG. **2**. At step **200**, the supervisor system generates magic packet directing waking-up of a target computer system, and the target computer system receives the magic packet via a network.

At step **210**, the target computer system generates a wake-up control signal if a network address contained in the received packet is the same as a network address of the target computer system, and transmits the wake-up control signal to a power management device installed in the target computer system. At step **220**, if the compared two network addresses are different from each other, the magic packet is discarded.

At step **230**, when the power management unit receives the wake-up control signal, power is supplied to a central processing unit (CPU) of the target computer system and a basic input/output system (BIOS) boots the system. At step **240**, an operating system (OS) is loaded.

However, in the aforementioned method of FIG. **2**, any computer system other than the supervisor system can generate a magic packet to access another computer system being suspended, so that a user with bad intentions may draw out information stored in another computer connected to his computer via a network or damage another computer system.

Turn now to FIG. **3**, which shows a block diagram showing the structure of a network connection portion of a computer system corresponding to a first preferred embodiment, in accordance with the principles of the present invention. Referring to FIG. **3**, a computer system having a remote wake-up function includes a magic packet controller **330** and a network information storage portion **340** as well as a network connection portion including a transformer **320**, a physical layer portion **310** and a network controller **300**. The network information storage portion **340** stores a network information including a network address and a password. Here, the network information storage portion **340** may be an electrically erasable and programmable read-only-memory (EEPROM).

The magic packet controller **330** receives a magic packet a via the physical layer portion **310**, compares a network address and a password contained in the magic packet a with the network address and the password stored in the network information storage portion **340**, respectively, and generates a wake-up control signal to transfer to a power management unit only when the compared addresses and passwords are the same as each other.

In FIG. **3**, even when the computer system is suspended, power is supplied to elements enclosed by dashed line indicated by reference numeral **20** from a switching mode power supply (SMPS).

With reference to switching mode power supplies, a switching mode power supply (SMPS) utilizing a pulse width modulator controls power of electronic machinery by performing a line regulation on the primary side of power and a load regulation on the secondary side of power by means of a pulse width modulation controller. Generally, switching mode power supplies require a protection circuit to protect the load, or to protect components within the power supply from an overvoltage, an overcurrent, or an induced surge. A switching mode power supply performs a line regulation by sensing the current from an output signal of a switching output part controlled by a pulse width modulation controller, performs a load regulation by detecting the voltage change induced from a coil of the largest turns ratio of the secondary loads of the power, and has the voltage of the power on the secondary side compensated in order to pass the results of the line regulation and the load regulation back to the pulse width modulation controller. A switching mode power supply may include an alternating current (AC) input part, a rectifier part, a switching transformer, a switching output part, a pulse width modulation controller, a current sensing part, an output part, and an error detection and feedback part. The alternating current input part receives an alternating s current voltage from an external source. Then the alternating current input part supplies the alternating current voltage to the rectifier part, which then outputs a direct current (DC) voltage to a load on the primary side of the switching transformer. The load in this instance is a primary coil. The switching transformer inputs the direct current voltage from the rectifier part. The switching transformer then induces different predetermined voltages to loads on the secondary side, each load having different turn ratios. The switching transformer induces the different predetermined voltages to the different loads by switching according to the control signal applied from a switching output circuit in the switching output part. The loads in this instance are coils. The output part includes a plurality of outputs for the purpose of rectifying and smoothing voltages induced into the loads, and then outputs different predetermined voltages. Each output of the output part constitutes a rectifying diode and a smoothing capacitor for rectifying and smoothing voltages induced on the loads of the switching transformer. An error detection and feedback part detects an error of the highest voltage, induced on the load having the highest turns ratio, output from the output part, and feeds back the detected voltage errors to the pulse width modulation controller. A switching output circuit in the switching output part, which is composed of a

switching element such as a field effect transistor (FET), controls on time and off time of the primary coil of the switching transformer by means of the pulse width modulation signal outputted from the pulse width modulation controller. A current sensing part senses an output current from the switching output circuit and supplies the sensed current to the pulse width modulation controller. One example where a tertiary side coil is utilized is as follows. The pulse width modulation controller inputs at least three signals: a voltage error detected by the error detection and feedback part, the output current of the switching output circuit sensed by the current sensing part, and a voltage induced on a tertiary coil of the switching transformer. Then the pulse width modulation controller outputs pulse width modulation signals to the switching output circuit in the switching output part with a duty cycle modulated in accordance with the three signals received by the pulse width modulation controller. The switching mode power supply senses an electric current from an output signal of a switching output part which is controlled by the pulse width modulation controller to perform the line regulation. The switching mode power supply detects a variation of voltage induced from a coil of one terminal among the loads at the secondary side of power to perform the load regulation. The results of the line regulations and load regulations are fed back to the pulse width modulation controller to thereby compensate the voltage at the secondary side of power.

With further reference to FIG. **3**, when the computer system is recovered to a normal state by the wake-up control signal, the network controller **300** accesses the network information stored in the network information storage portion **340** via the magic packet controller **330** to control transmission/reception of data via the network. Also, elements enclosed by dashed line indicated by reference numeral **10** in FIG. **3** may be implemented as an extra card or on-boarded on a main board of the computer system.

Turn now to FIG. **4**, which shows a block diagram showing the structures of a network connection portion and a basic input/output system (BIOS) of a computer system corresponding to a second preferred embodiment, in accordance with the principles of the present invention. Referring to FIG. **4**, a computer system having a remote wake-up function includes a magic packet controller **430**, a network information storage portion **440** and a BIOS **460** having a magic packet identification portion **463**, as well as a network connection portion **25** having a transformer **420**, a physical layer portion **410** and a network controller **400**.

In FIG. **4**, the network information storage portion **440** stores a network information d including a network address and a password. Here, the network information storage portion **440** may be an EEPROM. The magic packet controller **430** receives a magic packet c via the physical layer portion **410**, compares a network address and a password contained in the magic packet e with the network address and the password stored in the network information storage portion **440**, respectively, and generates a wake-up control signal to transfer to a power management unit only when the compared addresses and passwords are the same as each other.

With reference to FIG. **4**, the BIOS **460** has a power on self test (POST) portion **462** for performing a self test after power is supplied, and an interrupt handler **464** having a routine for processing interrupt. Here, the POST portion **462** has the magic packet identification portion **463** for transmitting an identification request packet to request identification of a magic packet to a supervisor system which has transmitted the magic packet, and for continuing to boot the computer system only when an identification packet has arrived from the supervisor system.

The BIOS **460** is connected to an industry standard architecture (ISA) bus, and the ISA bus connected to a Peripheral Component Interconnect (PCI) bus via a PCI-to-ISA bridge **450**. In FIG. **4**, even when the computer system is suspended, power is supplied to elements enclosed by dashed line indicated by reference numeral **40** from an SMPS. When the computer system is recovered to a normal state by the wake-up control signal, the network controller **400** accesses the network information d stored in the network information storage portion **440** via the magic packet controller **430** to control transmission/reception of data via the network.

Turn now to FIG. **5**, which shows a flowchart illustrating a remote wake-up method of the computer system shown in FIG. **3**, through identification of a password, corresponding to a preferred embodiment, in accordance with the principles of the present invention. A method for waking up the computer system shown in FIG. **3** according to a preferred embodiment of the present invention will be described with reference to FIG. **5**.

In FIG. **5**, at step **500**, the physical layer portion **310** receives the magic packet including the network address and the password via the network, and transfers the magic packet to the magic packet controller **300**.

At steps **510** and **530**, the magic packet controller **330** makes a determination as to whether or not both the network address and the password included in the magic packet are the same as those stored in the network information storage portion **340**. At step **520**, if the compared addresses or passwords are different from each other, the magic packet is discarded, stopping the waking-up process on the computer system.

In FIG. **5**, if the compared addresses and passwords are the same as each other, the magic packet controller **330** generates the wake-up control signal and transfers the wake-up control signal to a power management unit. At step **540**, the computer system is recovered to a normal state from a suspended state by the power management unit, power is supplied to a CPU, and the computer system is booted by a BIOS. At step **550**, an operating system is loaded.

Turn now to FIG. **6**, which shows a flowchart illustrating a remote wake-up method of the computer system shown in FIG. **4**, through identification of a packet, corresponding to another preferred embodiment, in accordance with the principles of the present invention. A method for waking up the computer system shown in FIG. **4** will be described with reference to FIG. **6**.

FIG. **6**, at step **600**, the physical layer portion **410** receives the magic packet including the network address and the password via the network, and transfers the magic packet to the magic packet controller **430**. At step **610**, the magic packet controller **430** makes a determination of whether or not only the network address included in the magic packet is the same as that stored in the network information storage portion **440**. At step **620**, if the compared addresses are different from each other, the magic packet is discarded, stopping the waking-up process.

In FIG. **6**, if the compared addresses are the same as each other, the magic packet controller **430** generates the wake-up control signal and transfers the wake-up control signal to a power management unit. At step **630**, the computer system is recovered to a normal state from a suspended state by the power management unit and power is supplied to a CPU, so that system initialization is performed by the POST portion **462** of the BIOS **460**.

In FIG. 6, at step 640, during the power on self test (POST), the magic packet identification portion 463 transfers an identification request packet to a supervisor system identified based on the address contained in the magic packet. Here, the identification request packet is transferred via the network controller 400, the physical layer portion 410, the transformer 420 and the network in sequence.

At step 650, after a predetermined time lapse, the magic packet identification portion 463 receives an identification packet from the supervisor system via the transformer 420, the physical layer portion 410 and the network controller 400 in sequence. Here, the identification request packet includes a random number set by a predetermined method, and the identification packet includes a secret code generated using the random number and a predetermined secret code generation function.

At step 660, the magic packet identification portion 463 compares the secret code of the identification packet with a secret code which is generated based on the random number and using the same secret code generation function as that of the supervisor system. At step 620, if the compared secret codes are different from each other, the magic packet is discarded, stopping the waking-up process on the computer system. At step 670, however, if the compared secret codes are the same each other, an operating system is loaded to operate the computer system. The secret codes can correspond to confidential information.

Turn now to FIG. 7, which shows a flowchart illustrating a remote wake-up method of the computer system shown in FIG. 4, through identification of a password and a packet, corresponding to still another preferred embodiment, in accordance with the principles of the present invention. A method for waking up the computer system shown in FIG. 4 will be described with reference to FIG. 7.

FIG. 7, at step 700, the physical layer portion 410 receives the magic packet having the network address and the password via the network, and transfers the magic packet to the magic packet controller 430. At step 710, the magic packet controller 430 makes a determination of whether or not both the network address and the password included in the magic packet are the same as those stored in the network information storage portion 440.

Then, steps 720 through 770 are performed, which are the same as the steps 620 and 670 described with reference to the flowchart of FIG. 6. Thus, a determination of whether or not the supervisor system is authorized can be made through two steps: identification using the network address and the password by the magic packet controller 430, and identification based on the identification packet by the magic packet identification portion 463.

The network 100 of FIG. 1 can correspond to a standard Ethernet network, a fast Ethernet network, or any other type of network linking a plurality of computer systems together and allowing those computer systems to share files and resources.

As described above, in the computer system having a remote wake-up function and the remote wake-up method thereof according to the present invention, when waking up remotely a computer system via a network, it is determined whether or not such remote waking up is by an authorized supervisor system. As a result, the computer system can be prevented from having information stolen therefrom or damage by a user with bad intentions.

While the present invention has been illustrated by the description of embodiments thereof, and while the embodiments have been described in considerable detail, it is not the intention of the applicant to restrict or in any way limit the scope of the appended claims to such detail. Additional advantages and modifications will readily appear to those skilled in the art. Therefore, the invention in its broader aspects is not limited to the specific details, representative apparatus and method, and illustrative examples shown and described. Accordingly, departures maybe made from such details without departing from the spirit or scope of the applicant's general inventive concept.

What is claimed is:

1. An apparatus, comprising:

a computer system processing first data when said computer system is in a first power mode, said computer system not processing the first data when said computer system is in a second power mode not corresponding to said first power mode;

a storage unit storing a first address and a first password;

a control unit being coupled to said storage unit and said computer system, said control unit receiving a first packet signal including a second address and a second password, comparing said first address and said first password with said second address and said second password respectively, and generating a control signal when said first address corresponds to said second address and said first password corresponds to said second password, said computer system being initialized in response to said control signal, said computer system being converted to said first power mode from said second power mode in response to said control signal;

a supervisory computer unit transmitting said first packet signal to said control unit;

a network unit being disposed between said supervisory computer unit and said computer system, said network unit coupling said supervisory computer unit and said computer system;

a confirmation unit being coupled to said computer system and transferring an identification request signal to said supervisory computer unit in response to said first packet signal received from said supervisory computer unit, said computer system having an operating system loaded onto said computer system when a second packet signal is received from said supervisory computer unit in response to said identification request signal.

2. The apparatus of claim 1, said first address corresponding to a network address of said supervisory computer unit.

3. The apparatus of claim 2, the operating system being loaded onto said computer system when data in said second packet signal satisfies a predetermined test.

4. The apparatus of claim 3, said second packet signal satisfying said predetermined test when a code received in said second packet signal corresponds to a generated code.

5. The apparatus of claim 2, further comprising a basic input output system coupled to said computer system, said basic input output system including a power on self test portion for performing said transferring of said identification request signal.

6. The apparatus of claim 5, said power on self test portion loading the operating system onto said computer system when said second packet signal is received from said supervisory computer unit in response to said identification request signal.

7. The apparatus of claim 1, said first address corresponding to a network address of said computer system.

8. The apparatus of claim 7, the operating system being loaded onto said computer system when data in said second packet signal satisfies a predetermined test.

9. The apparatus of claim 8 said second packet signal satisfying said predetermined test when a code received in said second packet signal corresponds to a generated code.

10. The apparatus of claim 7, further comprising a basic input output system coupled to said computer system, said basic input output system including a power on self test portion for performing said transferring of said identification request signal.

11. The apparatus of claim 10, said power on self test portion loading the operating system onto said computer system when said second packet signal is received from said supervisory computer unit in response to said identification request signal.

12. The apparatus of claim 11, said computer system receiving a first power when said computer system is in said first power mode, said computer system receiving a second power when said computer system is in said second power mode, said first power being more than said second power.

13. The apparatus of claim 11, further comprising a power unit supplying a low level of power to said computer system when said computer system corresponds to said second power mode, and supplying a high level of power to said computer system when said computer system corresponds to said first power mode, said high level of power corresponding to more power than said low level of power.

14. The apparatus of claim 11, further comprising a power unit not supplying power to said computer system when said computer system corresponds to said second power mode, and supplying power to said computer system when said computer system corresponds to said first power mode, said storage unit corresponding to one electrically erasable programmable read only memory.

15. A method, comprising:

supplying a first level of power to a first computer system;

receiving a first packet signal via a network unit, said network unit being coupled to at least said first computer system and a second computer system;

detecting whether a first network address contained in said first packet signal corresponds to a predetermined address;

detecting whether a first password contained in said first packet signal corresponds to a predetermined password;

when said first network address corresponds to said predetermined address and said first password corresponds to said predetermined password, supplying a second level of power to said first computer system and initializing said first computer system and not loading an operating system for operating said first computer system, said second level of power being higher than said first level of power;

when said first network address corresponds to said predetermined address and said first password corresponds to said predetermined password, transmitting an identification request signal to said second computer system from a power on self test portion of a basic input output system of said first computer system;

receiving an identification packet signal in response to said identification request signal;

determining whether said identification packet signal corresponds to a predetermined identification code; and

when said identification packet signal does correspond to said predetermined identification code, loading the operating system for operating said first computer system.

16. The method of claim 15, said initializing of said first computer system corresponding to performing a power on self test procedure on said first computer system by said basic input output system.

17. The method of claim 15, said first network address corresponding to said second computer system.

18. The method of claim 15, said first network address corresponding to said first computer system.

19. The method of claim 15, said second computer system corresponding to a supervisory computer system.

20. The method of claim 15, said identification packet signal corresponding to said predetermined identification code when said identification packet signal is received from said second computer system.

21. The method of claim 15, said identification request signal including a random number, said identification packet signal including a secret code, said secret code being generated based on said random number and being generated by a predetermined secret code generation function.

* * * * *

US006002427A

United States Patent [19]

Kipust

[11] Patent Number: 6,002,427

[45] Date of Patent: Dec. 14, 1999

[54] **SECURITY SYSTEM WITH PROXIMITY SENSING FOR AN ELECTRONIC DEVICE**

[76] Inventor: **Alan J. Kipust**, 41 W. 72nd. St., #4H, New York, N.Y. 10023

[21] Appl. No.: **08/929,479**

[22] Filed: **Sep. 15, 1997**

[51] **Int. Cl.**[6] **H04N 7/18**

[52] **U.S. Cl.** **348/156**; 348/634; 340/571; 340/573

[58] **Field of Search** 348/633, 634, 348/77, 819, 156; 340/679, 680, 522, 875.31, 825.34, 571.39, 573, 541, 565, 825.54; 395/188; 380/4, 25; 707/1, 9; H04N 7/18

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,628,315	12/1971	Bartholomew .	
3,736,729	6/1973	Peterson .	
3,863,196	1/1975	Hilles .	
4,039,853	8/1977	Koizumi et al. .	
4,133,506	1/1979	Webster	246/172
4,233,950	11/1980	Krolski et al. .	
4,566,688	1/1986	Monica .	
4,641,191	2/1987	Sutton .	
4,716,469	12/1987	Kim et al. .	
4,835,614	5/1989	Ryu .	
5,039,038	8/1991	Nichols et al.	340/825.5
5,044,472	9/1991	Dammeyer et al. .	
5,278,654	1/1994	Yang .	
5,406,261	4/1995	Glenn	340/540
5,453,644	9/1995	Yap et al. .	
5,495,302	2/1996	Abruna .	
5,505,528	4/1996	Hamman et al. .	
5,521,652	5/1996	Shalvi .	
5,541,580	7/1996	Gerston et al. .	
5,541,664	7/1996	Cuadrado .	
5,608,378	3/1997	McLean et al.	340/540
5,670,940	9/1997	Holcomb et al.	340/540
5,757,271	5/1998	Andrews	340/571
5,835,083	11/1998	Nielsen et al.	345/211

FOREIGN PATENT DOCUMENTS

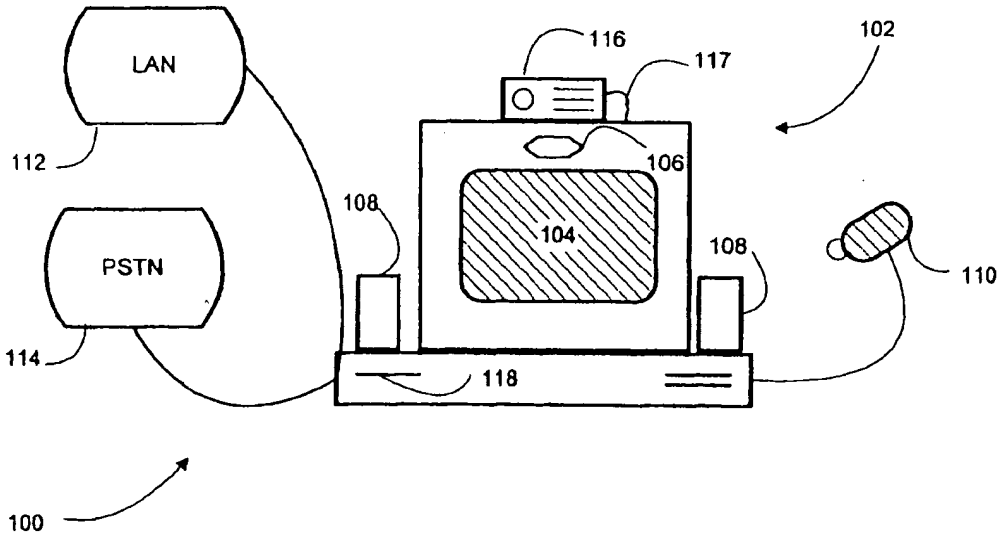
2176859	10/1990	Japan	15/30

Primary Examiner—Bryan Tung
Assistant Examiner—Nhon T. Diep
Attorney, Agent, or Firm—Charles G. Call

[57] **ABSTRACT**

A security system includes a proximity sensor to protect against unauthorized access to an electronic device. The security system is armed upon an input from the proximity sensor indicating departure of an authorized user from the vicinity of the electronic device. The security system provides commands to the electronic device as well as other devices coupled to the electronic device to sound an alarm in event of a security violation, clear a display screen of the electronic device or take other security measures to prevent unauthorized use of or access to information contained in the electronic device. The security system can include audio and video input devices to capture and store audio and video information while the system is armed and/or while a security violation is occurring. In certain embodiments, the security system also performs usage tracking of the electronic device.

25 Claims, 12 Drawing Sheets



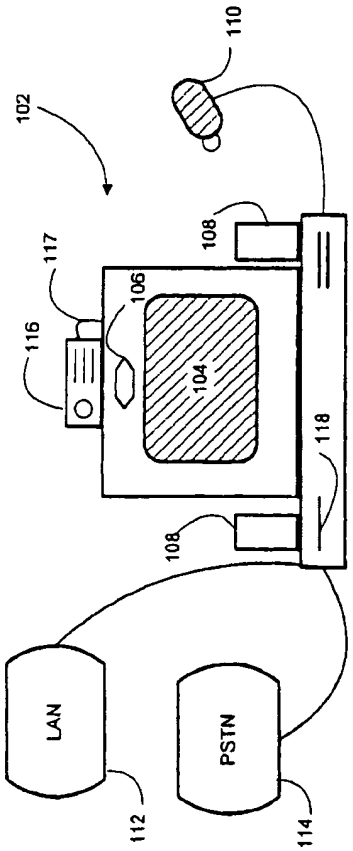


Figure 1

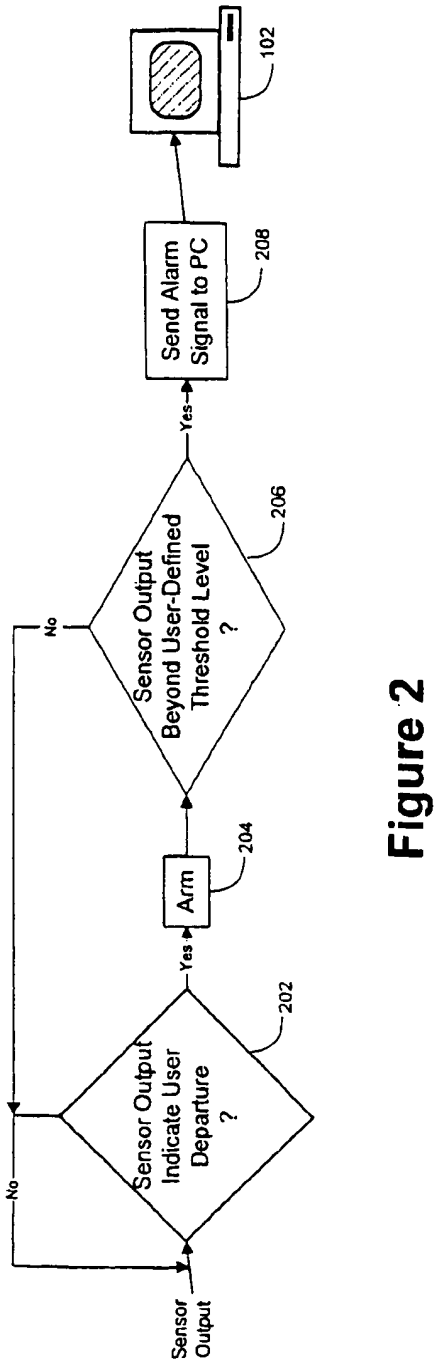


Figure 2

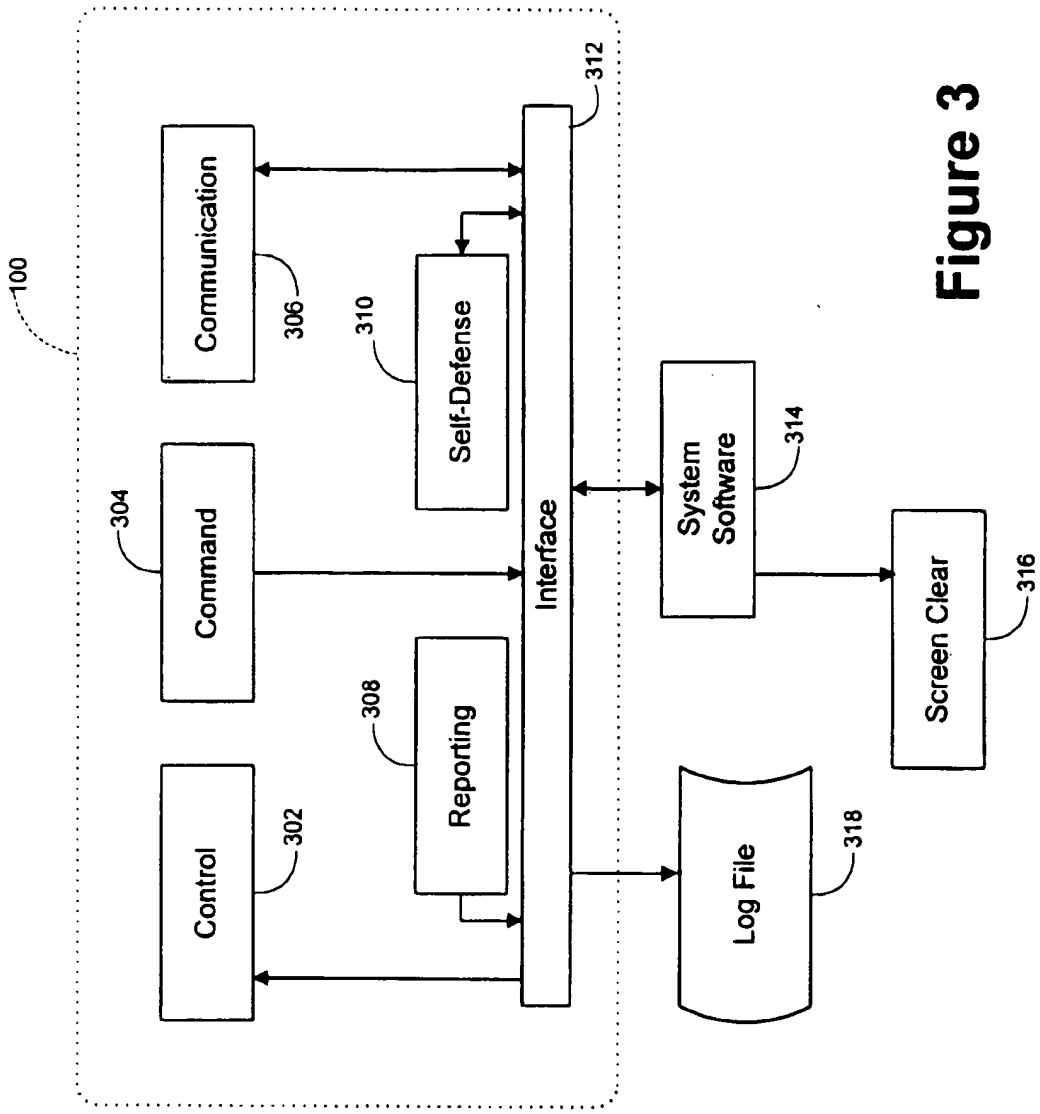

100
Communication
306
Self-Defense
310
312
Command
304
Interface
System Software
314
Screen Clear
316
Reporting
308
Control
302
Log File
318

Figure 3

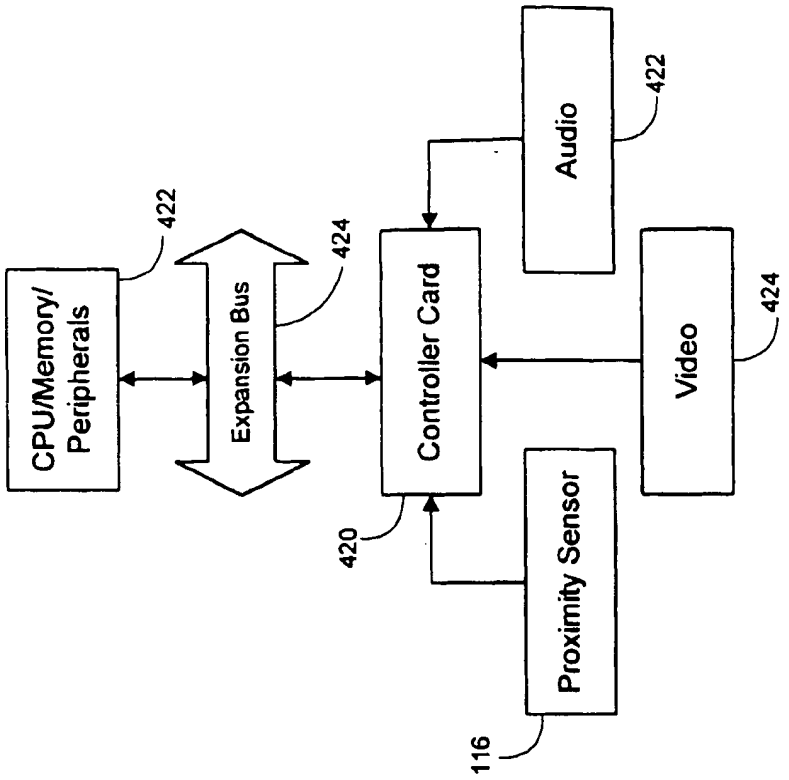


Figure 4B

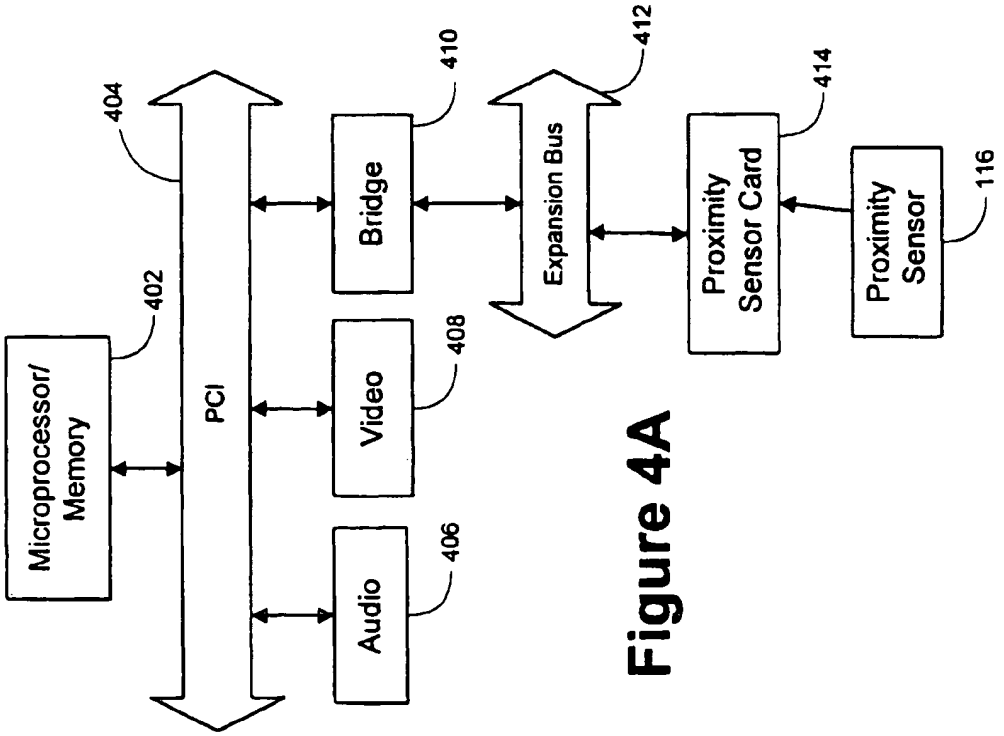


Figure 4A

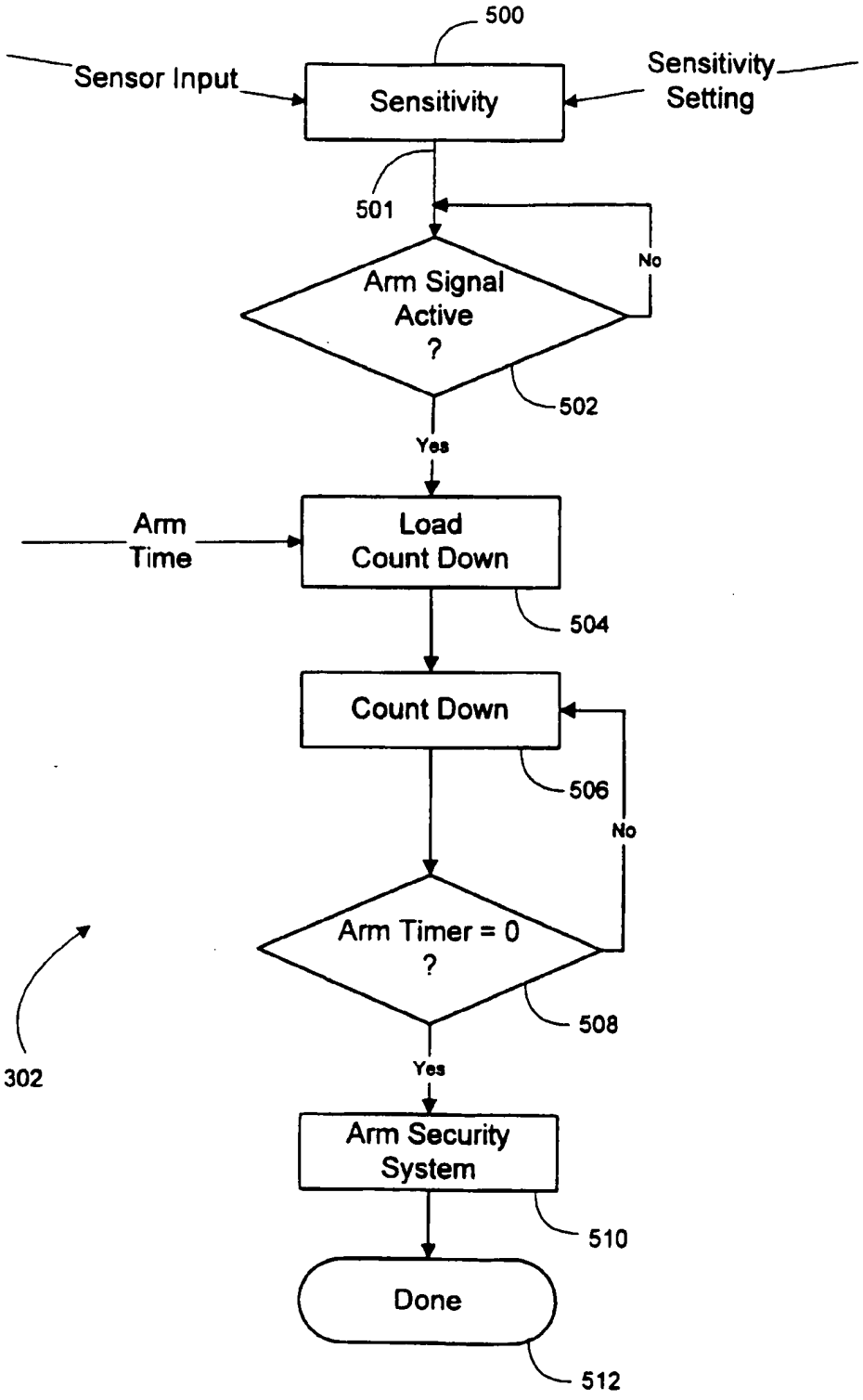

500
Sensor Input
Sensitivity
Sensitivity Setting
501
Arm Signal Active ?
No
502
Yes
Arm Time
Load Count Down
504
Count Down
506
No
Arm Timer = 0 ?
508
302
Yes
Arm Security System
510
Done
512

Figure 5

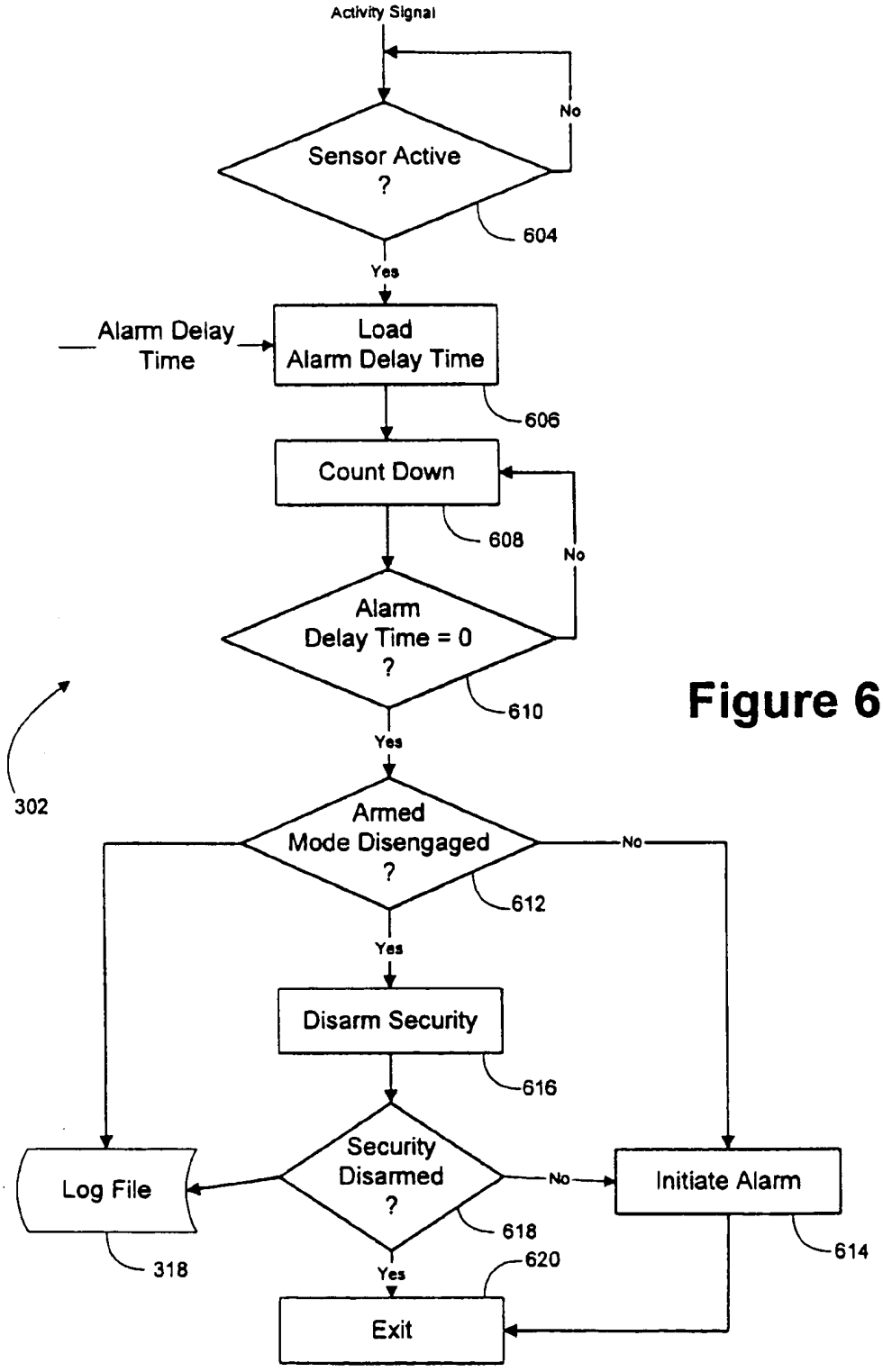

Activity Signal
Sensor Active ?
No
604
Yes
Alarm Delay Time
Load Alarm Delay Time
606
Count Down
608
No
Alarm Delay Time = 0 ?
610
Yes
302
Armed Mode Disengaged ?
No
612
Yes
Disarm Security
616
Security Disarmed ?
No
618
Yes
620
Log File
318
Initiate Alarm
614
Exit

Figure 6

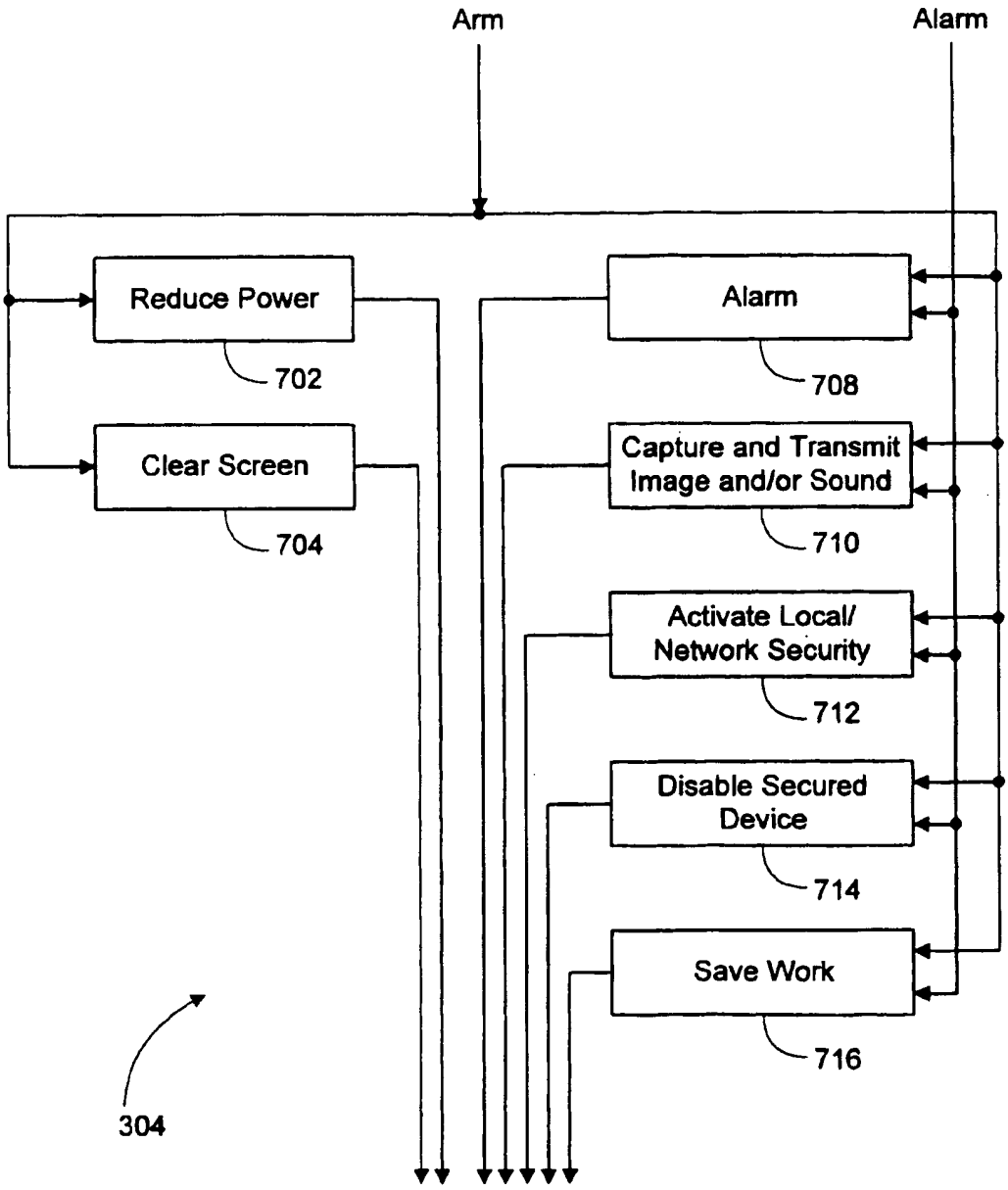

Arm
Alarm
Reduce Power
702
Clear Screen
704
Alarm
708
Capture and Transmit Image and/or Sound
710
Activate Local/ Network Security
712
Disable Secured Device
714
Save Work
716
304

Figure 7

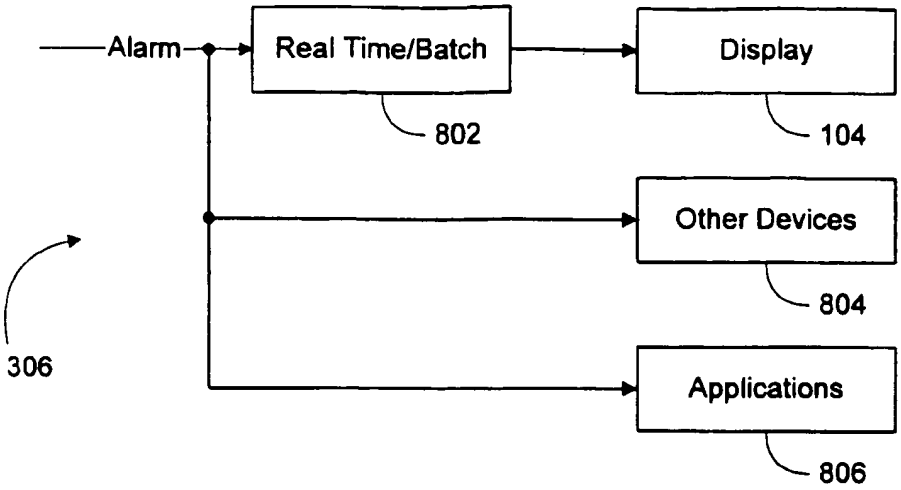


Figure 8

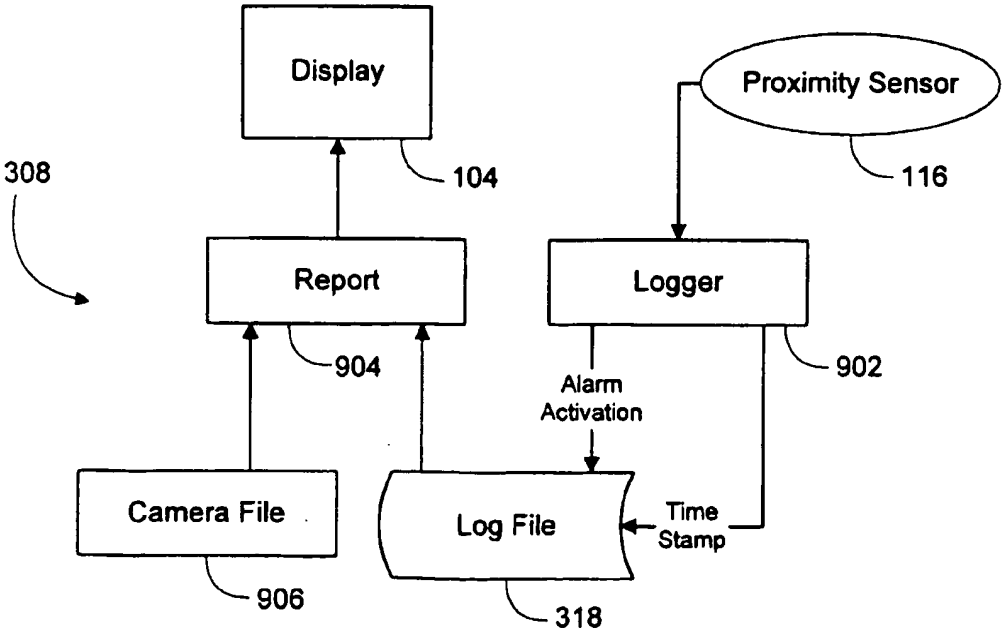


Figure 9

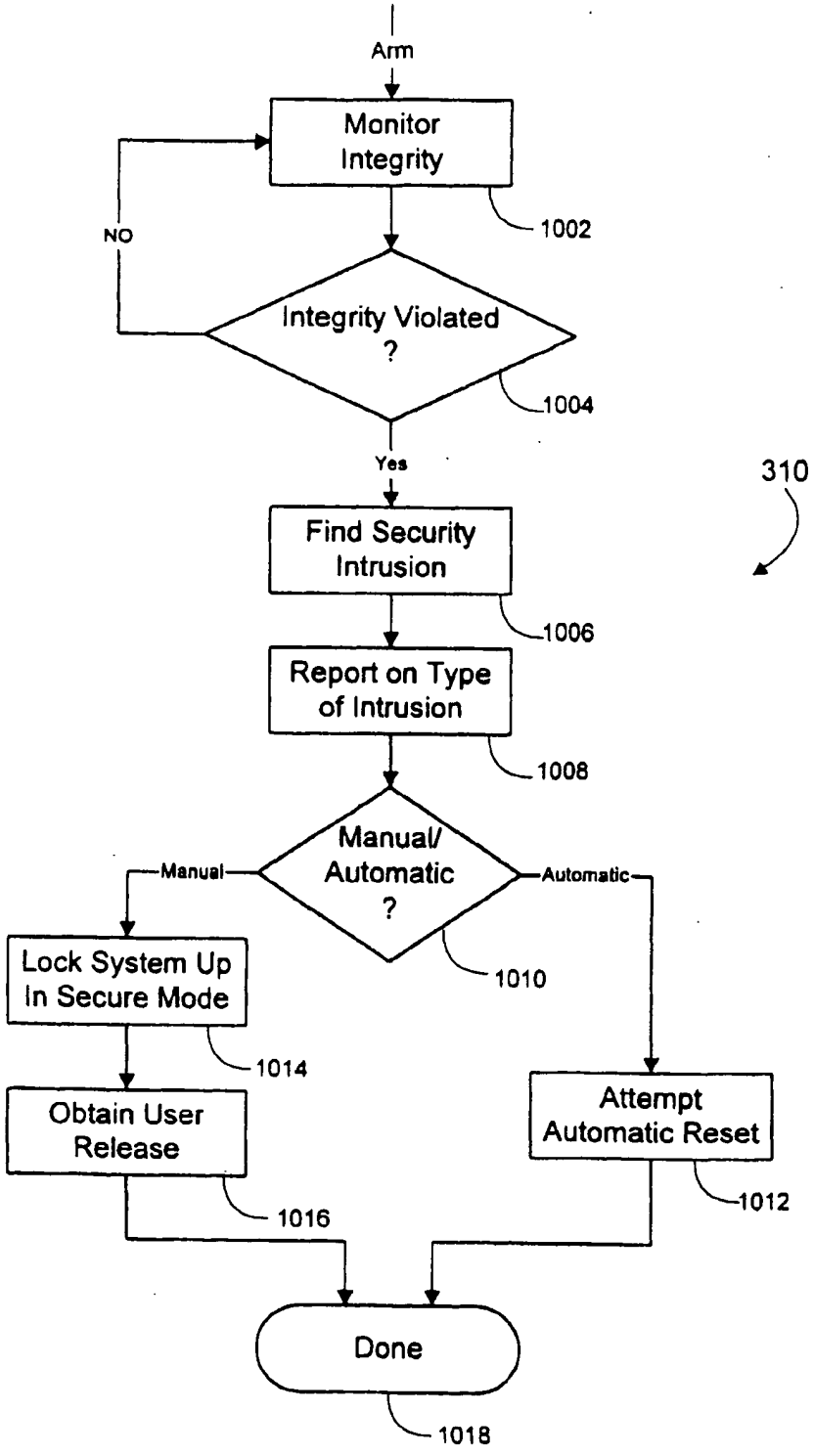

Arm
Monitor Integrity
1002
NO
Integrity Violated ?
1004
Yes
310
Find Security Intrusion
1006
Report on Type of Intrusion
1008
Manual/ Automatic ?
1010
Manual
Automatic
Lock System Up In Secure Mode
1014
Obtain User Release
1016
Attempt Automatic Reset
1012
Done
1018

Figure 10

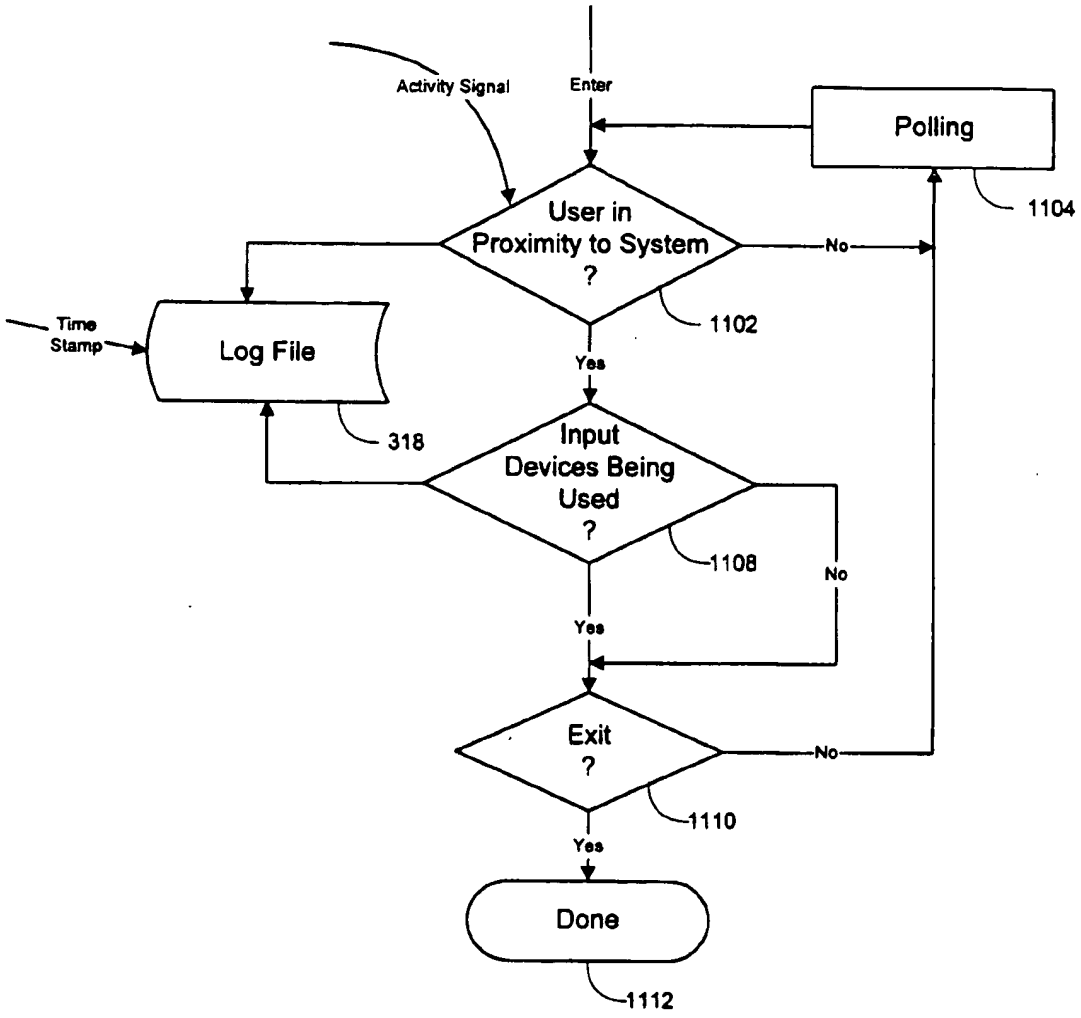

Activity Signal
Enter
Polling
1104
User in Proximity to System ?
No
1102
Time Stamp
Log File
Yes
318
Input Devices Being Used ?
1108
No
Yes
Exit ?
No
1110
Yes
Done
1112

Figure 11

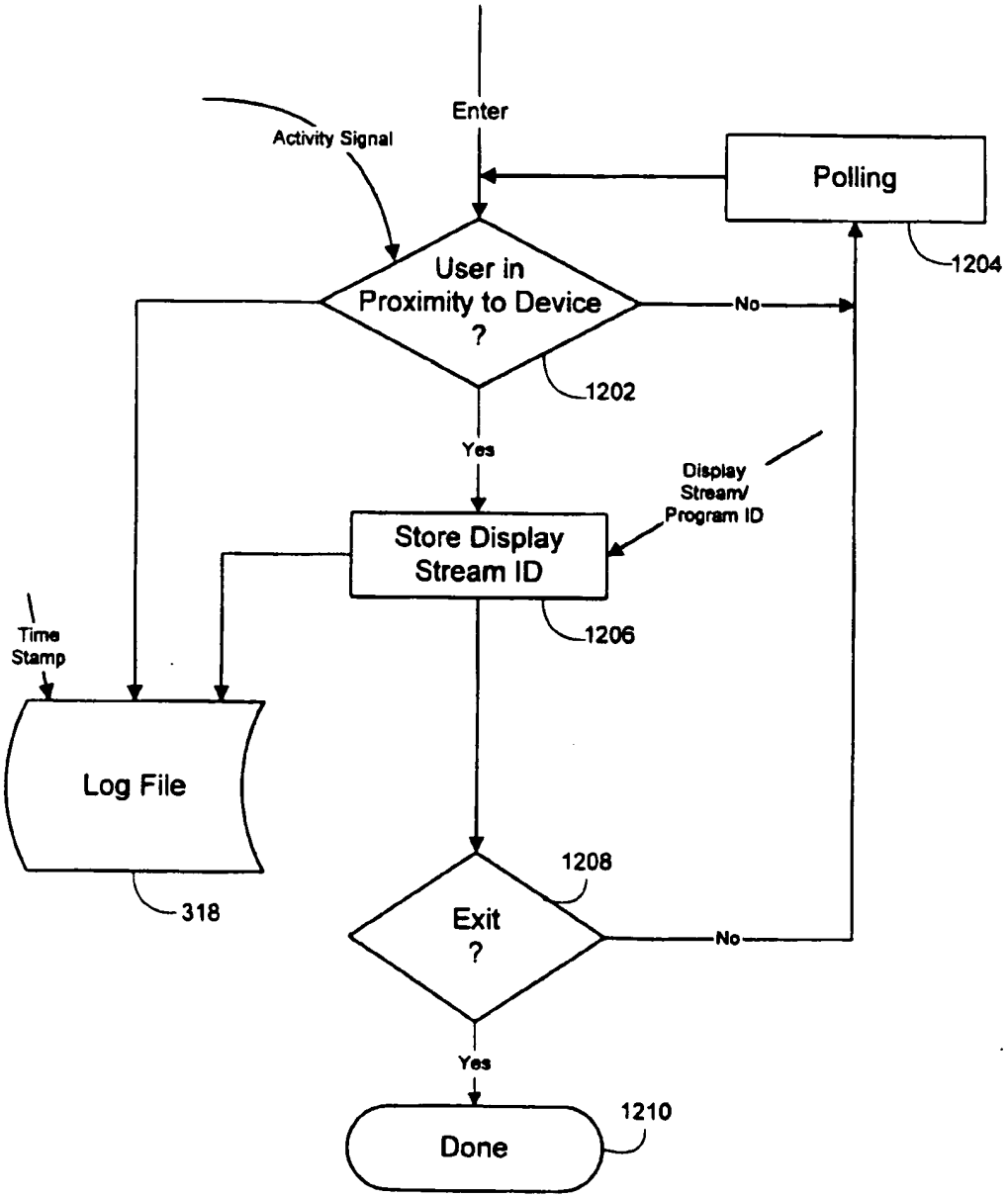

Enter
Activity Signal
Polling
1204
User in Proximity to Device ?
No
1202
Yes
Display Stream/ Program ID
Store Display Stream ID
1206
Time Stamp
Log File
318
1208
Exit ?
No
Yes
1210
Done

Figure 12

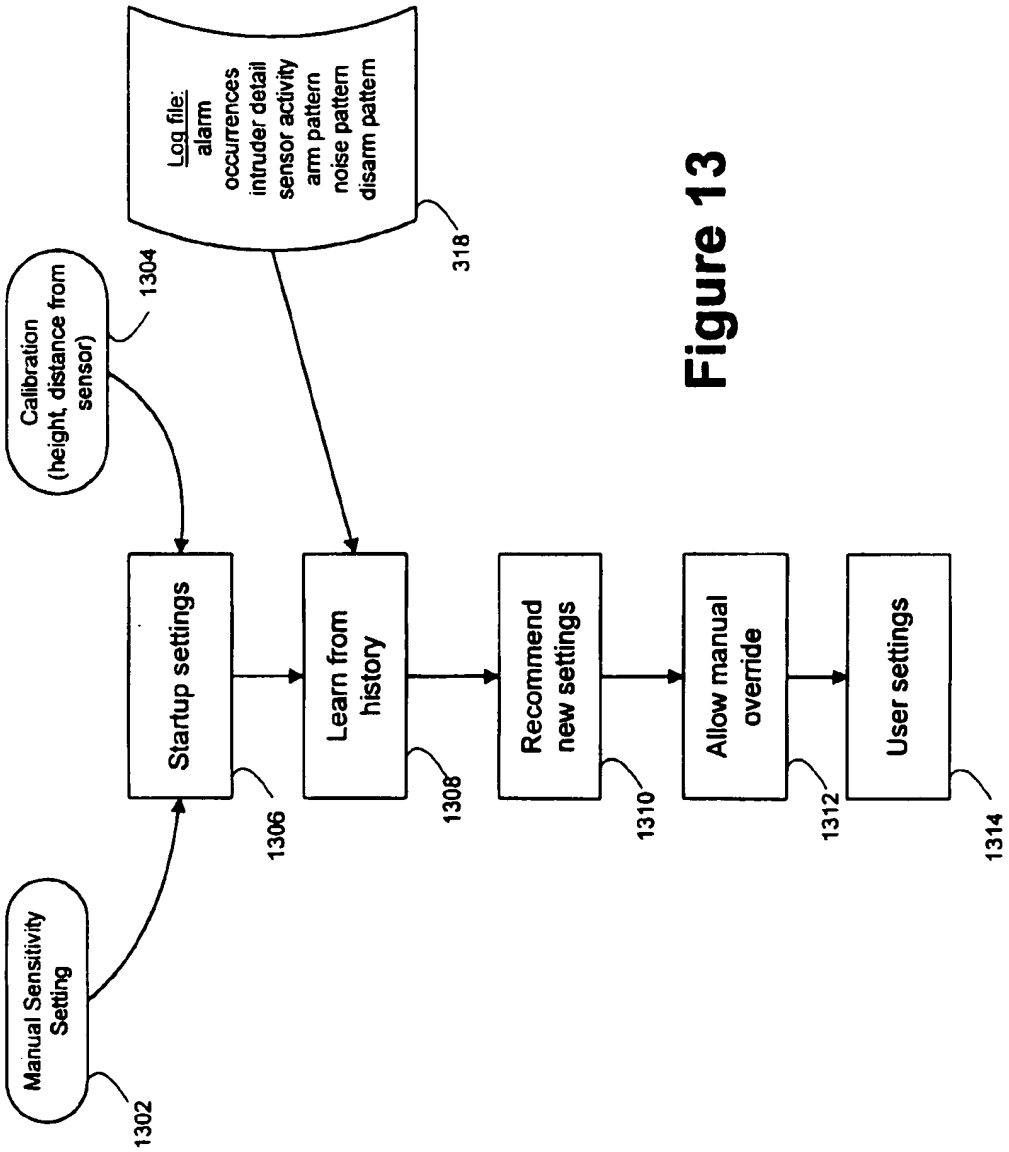

Log file:
alarm
occurrences
intruder detail
sensor activity
arm pattern
noise pattern
disarm pattern
318
Calibration
(height, distance from
sensor)
1304
Manual Sensitivity
Setting
1302
Startup settings
1306
Learn from
history
1308
Recommend
new settings
1310
Allow manual
override
1312
User settings
1314

Figure 13

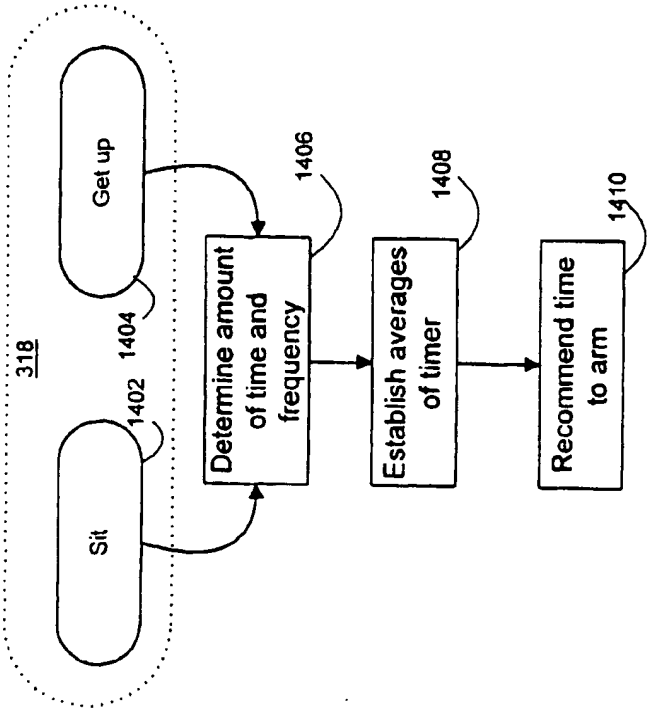


Figure 14A

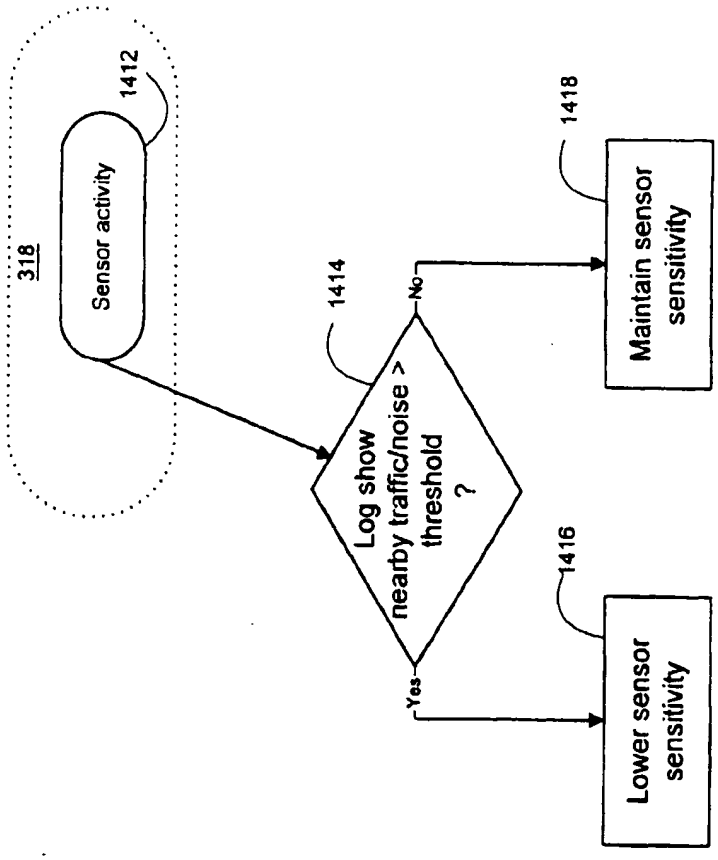


Figure 14B

SECURITY SYSTEM WITH PROXIMITY SENSING FOR AN ELECTRONIC DEVICE

FIELD OF THE INVENTION

This invention relates generally to the field of electronic security systems and more particularly to the field of electronic security systems for electronic devices.

BACKGROUND OF THE INVENTION

Computers and other related electronic devices have become important tools for the creation, manipulation, transmission and storage of sensitive information. Security mechanisms to prevent unauthorized use of computers or access to the information stored therein have accordingly seen increased use. The most common way of protecting unauthorized access to a computer and the information stored therein is by use of user accounts and passwords. In such systems, use of the physical machine or access to some or all data which may be accessed by the machine is prevented if the user is unable to enter the appropriate user account name and password.

A further popular security mechanism for computers is a screen saver program. Such programs, which were originally developed to prevent "burn-in" on Cathode Ray Tubes (CRT) have evolved into security mechanisms which prevent unauthorized use of a computer. Other security programs employing passwords are also available to protect against unauthorized use of a computer. Although programs requiring entry of passwords are the most popular and inexpensive form of protection for computers, other security mechanisms such as physical locks which prevent use of the computers input/output devices have also been developed.

Typically, screen saver or password type security programs, when activated, are invoked after passage of a certain amount of time when there has been no activity by the user (i.e. no inputs via input devices such as the keyboard or mouse) with respect to the computer. When invoked, the screen saver program typically replaces the image on the computer display with a moving image selectable by the user. In addition, the amount of time required to elapse before the screen saver is invoked is typically adjustable by the user. When the user later wishes to use the computer, an input device such as a keyboard or mouse may be used to cause the generation of an input region on the display into which the user enters an authorized password (typically the account name/number is automatically filled in). If the proper password is entered, the screen saver terminates and the image displayed prior to invocation of the screen saver is regenerated on the display, allowing full access to the device.

In using a password type security program to protect against unauthorized use of a computer, a user must make a decision between security and convenience. For the highest level of security, the time interval of inactivity required for invocation of the security program must be very small. However, a very small interval is highly inconvenient as most users are not constantly entering input into the computer. If a small interval is selected, the user will have to enter an input to prevent the security program from being activated, or will have to reenter the required password every time the passage of the small selected interval of time causes invocation of the security program.

Selection of a large time interval is more convenient but allows greater opportunity for unauthorized access to the computer. Consequently, a significant security/convenience trade-off must be made in the use of a conventional password type security program. This trade-off may be acceptable in environments where the users have physically enclosed spaces such as individual offices or cubicles where unauthorized individuals are less likely to enter. The trade-off may also be acceptable in environments where it is immaterial if information on a computer screen is viewed by others. However, in certain environments security is more crucial. For example, computers located on trading floors, banks or hospitals often contain sensitive and confidential information and are located in high traffic areas used by many unauthorized individuals. In such instances, security is of much greater concern. Moreover, often times users in such environments are less likely to have the time required to actively take security measures to protect against unauthorized use of secure machines or data.

As can be seen, there exists a need for an improved security system for electronic devices such as computers to protect against unauthorized use of the machine or access to the data accessible by the machine. It would be desirable for such a security system to prevent unauthorized access yet minimize inconvenience to or involvement by the user.

SUMMARY OF THE INVENTION

The present invention advantageously provides a security system for an electronic device which involves minimal routine involvement by the user of the device to invoke the protection provided by the security system. In a principle aspect, embodiments of the present invention employ a proximity sensor to detect the presence of a user at the secured device. When the proximity sensor detects that the user has left the device, the security system is armed to prevent unauthorized use.

Embodiments employing the principles of the present invention advantageously provide security with minimal involvement by the user. Such embodiments may be used in confidential environments such as trading floors, banks or hospitals where private or high-security information may be inadvertently displayed. Devices in home environments may also benefit by limiting access to certain electronic devices by children.

In a preferred embodiment, the security system takes the form of a system which protects against unauthorized use of a personal computer. The security system includes a proximity sensor to detect the presence and/or absence of a user at the device. A controller receives the output of the proximity sensor, filters the received signal according to a sensitivity setting and transmits an appropriate signal to the personal computer to invoke certain security measures such as clearing the screen of the information being displayed, invoking a screen saver and/or ignoring input from input devices such as keyboard or pointing device.

In certain embodiments, the security system receives inputs from audio and video devices to control operation of the system or to detect unauthorized use. In such embodiments, image or voice recognition programs are used to determine whether an individual in proximity to the protected device is an authorized user. Other embodiments contain reporting functions to allow reporting of security violations to other remotely located devices, to building security systems or to security personnel. Certain embodiments make extensive use of hardware and software contained in a personal computer, such as audio and video input and output devices, network connections, modems and system and application software. Other embodiments are more self-contained to provide the necessary hardware and software to implement a security system for devices which do not already contain the required components.

These and other features and advantages of the present invention may be better understood by considering the following detailed description of a preferred embodiment of the invention. In the course of this description, reference will frequently be made to the attached drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 of the drawings is a diagram of a electronic device in the form of a personal computer which employs the principles of the present invention;

FIG. 2 is a high-level flow diagram of the operation of a preferred embodiment;

FIG. 3 is a block diagram of functional modules of a preferred embodiment;

FIGS. 4A and 4B are alternative embodiments of hardware organizations of a personal computer as shown in FIG. 1 which employs the principles of the present invention;

FIGS. 5 and 6 are functional block diagrams showing operation of features of the control module of FIG. 3;

FIG. 7 is a functional block diagram showing greater details of the command module of FIG. 3;

FIG. 8 is a functional block diagram showing further details of the communications module of FIG. 3;

FIG. 9 is a functional block diagram showing further details of the reporting module of FIG. 3;

FIG. 10 is a flow diagram showing further details of the self-defense module of FIG. 3;

FIGS. 11 and 12 are flow diagrams showing operation of additional applications of the principles of the present invention;

FIG. 13 is a flow diagram showing operation of a dynamic sensitivity module of a preferred embodiment; and

FIGS. 14A and 14B are flow diagrams showing in greater detail portions of the flow diagram of FIG. 13.

DETAILED DESCRIPTION

FIG. 1 of the drawings shows an exemplary embodiment of a security system **100** which controls access to a secured device such as a personal computer (PC) **102**. The PC **102** takes a conventional form and includes a microprocessor, memory, long term storage such as a hard disk drive and an operating system. The PC **102** also includes input and output devices such as a keyboard and pointing device (not shown), a visual display **104**, a microphone **106** for accepting audio inputs and speakers **108** for generating audio outputs. The PC **102** may also receive video inputs from a video camera **110**. The PC **102** may also be coupled to a Local Area Network (LAN) **112** by way of an appropriate network controller (not shown) and to the Public Switched Telephone Network (PSTN) **114** by way of a modem or other suitable device (not shown).

The PC **102** is merely one example of an electronic system which may embody the principles of the present invention and the foregoing elements of the PC should not be construed as being limiting in any way. Other general purpose computing devices such as workstations which contain no long term storage, for example diskless workstations, may also be used. In addition, other electronic devices which operate in response to computerized controls, contained internally or externally to the device, may be considered to constitute a "secured device" as that term is used herein.

A proximity sensor **116** detects changes in heat, movement or other physical changes indicating user departure from an established vicinity of the PC **102**. Sensors for detecting such changes are well known and may respond to changes in heat, air pressure, movement by way of a variety of sensing technologies including laser, infrared or photo-electric technologies. Other sensors which detect changes in electric field may also be employed. An example of such a sensor is the Electric Field Proximity Sensor available from Russel Bik Design, San Luis Obispo, Calif.

Other types of sensors which may be used include those capable of reading or detecting an identification card carried by a user. Certain types of such sensors have the added advantage of being able to provide positive identification of the user by detecting a unique characteristic of the identification card. A variety of such identification cards are available and can be detected from different ranges. For example, proximity tokens which can be carried in a user's pocket, or cards which can be carried in a user's wallet or pocket are available from John Wainwright Systems Ltd, Bath Brewery, Bath, England.

The sensor **116** may also be a camera or microphone or physical key device used to access the computer. A sensor in the form of a camera operates in conjunction with conventional image recognition software to determine the presence of a user. A microphone operates in conjunction with audio recognition software to determine the presence of, for example, user sounds or user inputs via a keyboard, or overall user activity, such as the user's voice while speaking to others or on the telephone. The sensor **116** can also take the form of a deadman switch positioned in the chair or on the floor to detect departure from the secure vicinity near the PC **102**. While the user is in position, the deadman switch responds to the pressure or weight the user creates on the sensor. When the user departs, the pressure is relieved and access to the computer is terminated.

The proximity sensor **116** transmits a proximity signal to a controller **118** which controls operation of the security system **100**. The controller **118** may take the form of a card contained within the PC **102**, contained in a separate housing outside of the PC **102**. The controller **118** may also be implemented as software routines executed by the PC **102**. The sensor **116** is physically attached (by connector **117**) to the PC **102** in a manner to prevent unauthorized removal. Alternatively, the sensor **116** may be integral with the housing of the PC **102** or a peripheral to the PC such as the keyboard or pointing device. A separate sensor allows greater flexibility in the type of sensor used and in its placement. However, an integral sensor, such as in the display **104**, or the housing of the PC **102** or in peripheral devices external to the PC may lead to lower manufacturing costs in high volume applications. The sensor **116** may be coupled to the controller **118** by way of a wired or wireless link. Multiple sensors may also be employed to increase sensitivity, reliability or detection range.

FIG. 2 of the drawings illustrates general overall operation of the controller **100**. The controller receives a proximity sensor signal from the proximity sensor **116**, performs appropriate analog-to-digital (A/D) conversion and filtering, to eliminate spurious signals for example, and determines (**202**) if the sensor output indicates departure of the user. If user departure is not indicated then no action is taken. If the sensor output indicates that the user has departed, then at **204**, the security system is armed, meaning that certain security measures are undertaken to protect unauthorized access or use of the PC **102**. Once the system is armed, the controller tests at **206** to determine if the sensor output is greater than a user-defined threshold or sensitivity level. If not then no action is taken. If the sensor output is greater

than the user-defined threshold level then this is interpreted as an unauthorized use of the PC **102**. The controller responds by sending at **208** an alarm signal to the PC **102**. The alarm signal may result in occurrence of a number of different events, which are described in further detail in connection with the description of FIG. **7**.

FIG. **3** of the drawings illustrates a block diagram of the functional modules of the controller **100**. The functional modules include a control module **302**, a command module **304**, a communication module **306**, a reporting module **308**, a self-defense module **310** and an interface module **312**. The interface module **312** provides a common interface between the modules **302**, **304**, **306**, **308** and **310** and components of the PC **102** such as the system software **314** of the PC **102**. Specifically, the interface module **312** receives control inputs and data from the system software **312** and provides commands to system software **312** in order to use the resources of the PC **102** such as a screen clear program **316** which operates to remove potentially sensitive information from the display **104**. The PC **102** may also include other commercially available resources to perform other security functions such as, for example, locking access to input or storage devices of PC **102**. An example of such commercially available resources are those provided by the Norton Your Eyes Only™ program for Windows 95 available from Symantec Corporation, Cupertino, Calif.

The functional modules shown in FIG. **3** are preferably implemented as software routines executed by a conventional stored program computer such as PC **102** or by a separate controller such as explained below in connection with FIG. **4B**. In an exemplary embodiment, the system software **314** is provided by the Windows 95 operating system available from Microsoft Corporation, Redmond, Wash. The screen clear program **316** is also supplied by the Windows 95 operating system which includes a screen saver program selectable by the user. The Windows 95 operating system manages system resources such as storage devices, handles input from input devices and handles writing to output devices such as displays and printers. Preferably, the functional modules shown in controller **100** make use of such services provided by Windows 95 by way of calls to the operating system which will be understood to those skilled in the art in view of the present disclosure.

The control module **302** receives inputs, by way of interface **312**, to control functions such as arming and disarming of the system, and sensitivity of the proximity sensor inputs. The command module **304** provides commands to portions of the security system **100** and PC **102** to perform functions such as sounding an alarm in event of a security violation, reducing power to portions of the PC **102** when the security system is armed, clearing the screen of information when the system is armed, invoking a screen saver, disabling the PC **102**, saving recent work done on the PC **102**, activating a screen saver and capturing video and audio inputs while a security violation is in progress. These and other features are further explained below in connection with FIG. **7**.

The communications module **306** provides status information to other machines, alarm systems or security personnel. The communications module is explained in further detail in connection with FIG. **8**. The reporting module **308** stores information to log file **318** regarding events when the system is armed and when security violations are taking place. The log file **318** may be stored in a hard disk drive of the PC **102**. Alternatively, the log file **318** may also be stored in a controller card in an implementation such as set forth in FIG. **4B**. The reporting module is explained in further detail below in connection with FIG. **9**. The self-defense module **310** monitors integrity of the security system **100** while the system is armed. If any aspect of the system is compromised without proper authorization, the self-defense module causes audible and visual alarms to be activated. The self-defense module is explained in further detail below in connection with FIG. **10**.

FIGS. **4A** and **4B** show alternative embodiments of implementations of the controller **100** for use in PC **102**. In FIG. **4A**, the controller **100** is implemented by extensive use of components and functions supplied with many personal computers. A personal computer in the embodiment of FIG. **4A** has contained therewith components commonly found in modern computers, including, a microprocessor and memory **402** coupled to a standard bus such as the PCI (Peripheral Components Interconnect) bus **404**. Also coupled to the bus **404** are audio and video controllers **406** and **408** to implement audio and video input and output. A bridge **410** couples the components on the bus **404** to components on a conventional expansion bus **412**. The expansion bus **412** has coupled thereto a proximity sensor card **414** which receives inputs generated by proximity sensor **116**. The proximity sensor **116** and card **414** may be eliminated if the proximity sensor takes the form of a video camera or microphone with appropriate recognition software. In such an instance, the audio and video components **406** and **408** would provide the necessary hardware.

FIG. **4B** shows an alternative configuration of the controller **100** in which the hardware necessary to implement the controller is contained on a separate controller card **420**. Such an embodiment is preferable for computers which do not have the hardware necessary to implement all of the functions required for the security system **100**. For example older computers may not have the sophisticated audio and video input and output systems available in many newer computers. In such an instance, the embodiment of FIG. **4B** may be preferable, as it contains on a single card the connections and components necessary to add the functions to the PC **102** to implement the security system **100**. As seen in FIG. **4B**, the PC **102** includes the necessary CPU, memory and peripherals **422** and an expansion bus **424**. Controller card **420** is coupled to the expansion bus **424** to communicate with the PC. The controller card **420** contains a microcontroller, random-access memory (RAM) for short term storage, long term program storage memory such as a Read-Only Memory (ROM) and input-output circuitry to accept inputs from a proximity sensor **116**, and audio inputs from an audio input device **422** and video inputs from a video input device **424**. The controller card **420** may also contain long term memory to store the log file **318**. Such memory may take the form of memory which is fed by a battery power supply or an alternative form of memory not requiring electrical power for storage of data, such as an Electrically Erasable Programmable Read Only Memory (EEPROM).

Alternatively, the embodiment of FIG. **4B** may be implemented on a card contained in a housing external to the PC **102**. Such a card would be coupled to the PC **102** via a port of the PC **102**. The controller card **420** and the sensor **116**, and audio and video modules **422** and **424** shown in FIG. **4B** are well suited to a PC **102** which does not have the audio and video hardware and software necessary to implement desired audio and video functions of the security system **100**. However, the controller card **420**, sensor **116**, and audio and video modules **422** and **424** may also be used in a PC **102** having a configuration such as shown in FIG. **4A**. FIGS. **4A** and **4B** show two examples of how a controller **100** may

be implemented for systems which have different hardware configurations. The hardware organizations shown in FIGS. 4A and 4B should not be construed as limiting in any way. The exact implementation of the functional modules shown in FIG. 3 is not critical. Variations in the hardware organizations shown in FIGS. 4A and 4B are well within the principles of the present invention. For example the hardware organizations shown in FIGS. 4A and 4B can be expected to change as ever more functions are integrated onto a single chip such as integration of certain or all of the audio and video functions together with the microprocessor. Other changes include, but are not limited to, the interconnection of the various components within the PC **102** by way of different bus structures.

FIGS. **5** and **6** are flow diagrams showing operation of the control module **302**. FIG. **5** shows the sequence of steps performed in arming the security system **100** to detect unauthorized use of the PC **102**. The steps in FIG. **5** illustrate in further detail the arm function shown at **204** in FIG. **2**. The controller **118** waits a pre-programmed amount of time before arming itself upon detection by the proximity sensor that the user has departed the work area. The user may occasionally walk away from the secured device for only seconds and there is no need to arm the security system. The user may set the most appropriate amount of time away from the computer that constitutes a true and permanent departure from the work area. This feature also allows the user to take into account the security needs for a particular machine. Thus, stricter security measures will require a smaller pre-programmed amount of time.

Turning to FIG. **5**, at **500** a signal generated by the proximity sensor **116**, which has been digitized and filtered as necessary, is received and compared against a sensitivity setting to generate an activity signal **501**. The sensitivity setting is selected by the user to adjust the sensitivity or range of the proximity sensor. Thus the vicinity in which an unauthorized intrusion is detected can be varied depending upon the security needs and environment of the secured device **102**. If the sensor signal received by sensitivity block **500** exceeds the sensitivity setting then the arm signal is generated to indicate that the user has departed the vicinity of the secured device. If the activity signal **501** indicates continuing activity in the vicinity of the secured device then no action is taken. If the activity signal indicates that activity has ceased then at steps **504**, **506** and **508** a count down procedure is performed to wait a pre-programmed amount of time before arming the security system. At step **504** a count down value is loaded with an arm time value, which is selected by the user. The controller then repeats steps **506** and **508** until the arm timer value has counted down to zero at which point at step **510** the security system is armed, and the arm routine is exited at step **512**.

The level or type of signal required to generate the activity signal **501** can advantageously be dynamically changed to account for differing levels of activity at different times of the day or different days of the week. For example, the activity signal **501** may be generated in response to a sensor input at a certain time of the day, say for example at nighttime, but not be generated in response to exactly the same signal at a different time of day, for example business hours in an office where the level of activity around the secured device is greater. FIG. **13** shows a flow diagram of operation of an embodiment of a dynamic sensitivity routine which performs such a function. Initially, a plurality of settings such as a manual sensitivity setting **1302** for the sensor **116** are used to generate startup settings **1306** for the system. Depending upon the type or types of sensor(s) used, calibration settings **1304** necessary for such sensors may also be used as inputs. The startup settings **1306** art then modified at **1308** in response to a variety of sensed information and new settings (**1310**) are then recommended. These settings can then be accepted or overridden (**1312**) to generate final settings **1314**. The modification, or learning, of the settings at **1308** is advantageously performed in response to information stored in log file **318**. Depending upon the configuration of the system **100**, the log file **318** can contain a wealth of information including the time and type of alarm occurrences, details as to any intruders such as video or audio information, the frequency and type of sensor activity, for instance the intensity of the signal generated by the sensor, the frequency and duration of arming of the system **100**, the patterns background noise detected by any sensors, and the frequency and duration of disarming the system **100**. Preferably such information is stored together with time and date information to enable a determination of particular times during the day and what days during the week in which particular activity occurs.

FIGS. **14A** and **14B** show two examples of the operation of learning block **1308**. In FIG. **14A**, a determination is made at **1406** of how often and for how long a user is sitting at the secured device based upon information stored in log file **318**. For purposes of clarity, this information is shown as being stored specifically in the form of information denoting when the user sits or gets up from the secured device. However, it should be understood that the information in the log file **318** may be stored in a number of formats and is likely to be stored in the form of raw data from sensors which has been digitized and filtered and time and date stamped. In such a case, such data is retrieved from the log file **318** and a determination is made from such data as to when the user was seated at the secured device, when the user got up to leave the vicinity of the secured device and when the user returned to the vicinity of the secured device. Once the frequency and amount of time for being seated at the secured device and being away from the secured device is determined, an average of such data is made and based upon such average, a new time required to elapse before the system is armed upon departure of the user from vicinity of the secured device is recommended. Other values providing an indication such as moving averages, mean time at the secured device or the like may be used as an alternative to using an average value.

FIG. **14B** shows an example of determination of a sensor sensitivity setting based upon sensor activity, such as proximity sensor **116**. At **1414**, sensor activity data **1412** stored in log file **318** is retrieved and analyzed to determine if the data shows noise or traffic in the vicinity of the secured device to be greater than a user adjustable threshold. Such analysis can be performed in a variety of ways. For example, an average of the sensor data can be taken, or a weighted average, with certain times of day, or certain types of sensor readings, being weighted differently than others. Other useful figures may include a median value of the readings or other like statistical quantities. If the traffic or noise in the vicinity of the secured device is found to be greater than the threshold then the sensitivity setting can be lowered to increase the sensitivity of the sensor. If the traffic or noise in the vicinity of the secured device is found to be less than the threshold then the sensitivity can be maintained.

FIG. **6** shows the sequence of steps performed in disarming the security system **100**. The user will need a few seconds to disarm the security system upon returning to the secured device. The security system advantageously allows an alarm delay time to be entered to control the amount of

time allowed to disarm the system. Ideally a minimal amount of time will be programmed to allow the user to disarm the system. This will leave the secured device exposed for the shortest amount of time should an intruder attempt to disarm the system. In FIG. **6** at **604**, the activity signal **501** is received and a test is performed to determine if the sensor has detected an authorized or unauthorized user in the work area. If no activity is detected then no action is taken. Otherwise if activity in the vicinity of the secured device is detected then at step **606** the alarm delay time value, selected in advance by the user, is loaded and at steps **608** and **610** a count down procedure is performed to allow the alarm delay time to elapse. Once the alarm delay time has elapsed, at **612**, a test is performed to determine if a proper attempt to disarm the system has been performed. By way of example, the system may be disarmed by entry of a password, or by pressing a predetermined sequence of keys on the keyboard or moving the pointing device in a particular manner. If a proper attempt to disarm the system has not been performed at the expiration of the alarm delay time, then at **614** an alarm mode is initiated. Otherwise, if a proper attempt at disarming the system has been made then at **616** an attempt is made to disarm the security system. It is possible that the security system is not disarmed after step **616**, for example because of failure of certain components. Thus at step **618** a test is performed to determine if the security system has actually been disarmed. If so, then the routine is exited at step **620**. If not, then the alarm is initiated at step **614**. The result of the test at step **618** is saved to the log file **318**.

FIG. **7** shows the commands implemented by the command module **304**. The command module **304** responds to an arm signal, such as generated by block **510** in FIG. **5**, indicating that the system is being armed, and the alarm signal, such as generated by block **614** in FIG. **6**. Modules **702** and **704** respond to the arm signal, module **708** responds to the alarm signal and modules **710**, **712**, **714** and **716** respond to the arm signal and the alarm signal. The functions performed by the modules shown in FIG. **7** are preferably selectable in advance to customize the security system for a particular environment.

Module **702**, upon arming of the system, causes a low power command to be issued to place the secured device in a low power mode. If the secured device takes the form of a personal computer then a number of options are selectable. For instance, the monitor can be dimmed or turned off, the processor speed can be decreased, the hard disc drive can be turned off or slowed, or the read/write head can be placed in the park position. Such power reduction modes are common in many personal computers and such modes can be activated under control of the power control module **702**.

Module **704** causes the screen of the secured device to be cleared to remove any secure information which may have been on the screen when the system was armed. This can be performed very simply by replacing the image on the screen with a new, predetermined image. The manner is which information is removed from the screen is selectable. Other options for removing information from the screen include closing any windows which may be open to display the background or desktop image found in graphical user interfaces or invoking a screen saver or other similar type of application program stored in the PC **102** or downloaded from another machine such as a server in response to a request by the PC. Screen savers are standard in many personal computers and several are typically supplied with the Windows 95 operating system which is generally installed on new personal computers. Module **704**, if activated, causes invocation of a pre-selected program such as a screen saver when the system is armed. Other programs which cause removal of information from the screen are also commercially available and, if installed, can be selected to be invoked by the module **704**.

Alarm module **708** responds to the alarm signal by causing an alarm to be activated. The type, number or level(s) of alarm(s) activated will differ depending upon the configuration selected for the system. For example, an alarm configuration for the system can include a simple bell, siren or other type of audible alarm, or voice recording, indicating a security violation. The alarm can also take the form of a visual indication such as a flashing light or can be a combination of audible and visible indications. Another alarm configuration includes different alarms for different types of security violations. For example a first type of visible alarm, or low level audible alarm can be activated in response to a minor security violation and a loud audible alarm can be activated in response to a security violation considered to be more serious.

Module **710** responds to arming of the security system by capturing audio and/or video information in the vicinity of the secured device. The captured information is digitized and stored in a conventional format in an appropriate storage device. In addition, the information can be transmitted live to a remote device for live viewing or listening. Video information can also be displayed on the display **104**. This feature allows anyone in the vicinity of the secured device **102** to be informed that a video recording is being made of their activity around the secured device. Module **710** can be selected for operation only when a security violation has occurred. In such a case, audio and/or video information is recorded only in response to the alarm signal, i.e. when a security violation has occurred.

Module **712** responds to arming of the security system by transmitting a command to cause activation of security measures to network **112** or to cause activation of other building security measures. Network security measures include increased security measures such as limiting access to certain files or directories of files in the file system to the system administrator or a limited number of authorized users. Other security measures include duplication of certain files or directories of files to preselected storage devices.

Module **714** disables the secured device **102** to prevent or limit further use. For example, the display **104** can be powered down or disabled, the input devices can ignore any further inputs until entry of a predetermined set of inputs or resetting of the secured device, or long term storage devices can be prevented from further modification of any data stored therein. Alternatively, the entire secured device can be powered down to prevent further operation. Some or all of the foregoing operations can be performed in response to the arm signal or the alarm signal.

Module **716** causes any data stored in temporary storage areas of the secured device to be stored to an appropriate file and causes any open files to be closed. Such files may be stored in long term storage devices in the secured device or to files stored elsewhere in network **112**. Module **716** operates in response to the arm signal or the alarm signal.

FIG. **8** shows details of operation of the communication module **306**. In response to the alarm signal, the communication module transmits information regarding intrusion to the display **104** of the PC **102**, to other devices **804** coupled to the PC **102**, and also to other applications **806** currently being executed by the PC **102**. The information transmitted by way of transmission module **802** is selectable by the user

or system administrator and can be transmitted in real time or in batch mode at selectable intervals. The other devices **804** include a system administrator terminal, all other computers proximate to the PC **102** or selected machines remote from the PC **102**. The information sent to other applications **806** is in the form of a command to save the data in files opened by the application and/or to exit the application.

FIG. **9** shows details of operation of the reporting module **308**. The reporting module **308** performs a logging function and a reporting function. The logging function is implemented by way of a logger **902** which receives a value indicative of the signal transmitted by the proximity sensor **116**, generates a time stamp and stores the information to log file **318**. The logger also stores the occurrence of an alarm to the log file together with a time stamp.

Report module **904** retrieves information from the log file **318** and generates a report for display on display **104**. If a camera is coupled to the PC **102** to generate video type data for a camera file **906**, the report module **904** contains the functionality necessary to cause retrieval and display of the data contained in the camera file **906**.

FIG. **10** shows further details of the operation of self-defense module **310**. The self-defense module responds to the arm signal by performing periodic integrity monitoring, steps **1002** and **1004**, of the system. This may be performed by performing checks of the input/output devices to ensure they are properly connected to the PC **102**. Monitoring of the input devices may also be performed to determine if access to the PC **102** has been attempted. For example, any use of the input devices can be construed as a security intrusion. A legitimate attempt to disarm the system is handled in a manner described in connection with FIG. **6**. Specifically, step **1004** can contain a delay time, such as shown at steps **606** and **608** in FIG. **6**, to ignore inputs which result in disarming of the system. If integrity of the system is determined to have been violated, then at **1006** the source or sources of the security intrusion is/are identified and at **1008** and the source or sources is/are reported at step **1008** in a manner described above in connection with FIG. **8**. At steps **1010**, **1012**, **1014** and **1016** a manual or automatic reset of the system is performed depending upon the type of reset selected. If an automatic reset of the system has been selected, then at step **1012**, an automatic reset of the system is attempted. If a manual reset has been selected, then at step **1014**, the system is locked so that no further use may be made. For instance, all inputs can be ignored until the system is properly disarmed at step **1016**.

FIGS. **11** and **12** show additional applications of the security system **100**. FIG. **11** shows an implementation in which the security system **100** is used to monitor usage of a computer based on timed utilization of the computer and proximity to the computer while not operating the computer. Such an implementation is particularly useful in environments where computers are rented such as at commercial copy shops, or in hotel or airport office facilities used by business travelers. Additional uses include data gathering to determine the usage pattern of a machine.

In FIG. **11**, the system loops between steps **1102** and **1104** periodically checking if the proximity sensor has detected activity in the vicinity of the secured device. If a user is detected to be in proximity to the secured device then at step **1108** a test is performed to determine if any input devices are being used. The result of the test is stored to the log file **318**, which also receives a time stamp to be stored with the information received from step **1108**. Next, a test is performed at **1110** to determine if the routine should be exited. This occurs, for example, in response to an input received, for example, from a system administrator, or upon expiration of a predetermined period of time. If no exit command has been received, then the routine returns to step **1104**, otherwise the routine is exited.

FIG. **12** shows an application in which the security system **100** is used to track usage of a secured device by monitoring the content of material being viewed on the secured device. For example, the content of programs being viewed on a television, or on a computer used as a television. Such an embodiment finds particular use to perform tracking of popularity of certain programs. For example, a television coupled to a system employing the principles of the present invention can be monitored to determine the video programs being viewed. In addition, a computer such as PC **102** can be monitored to determine the frequency of use of the computer programs executed by the PC. Alternatively, the content of information being downloaded to the PC **102** from remote sites such as from the Internet or from commercial databases can be monitored. In addition to tracking the content of material being viewed on the secured device, the identity or category of viewer can also be tracked. For example, if the PC **102** is appropriately configured with a camera and appropriate image recognition software then the identity or type of individual in proximity to the secured device can be determined. For example, comparisons can be made against a database to determine either the precise identity of the detected individual or the visual characteristics of the individual such as adult/child or male/female based on certain visual characteristics such as height and overall size of the individual, manner of dress, accessories and the like.

In FIG. **12**, a polling loop similar to that shown in FIG. **11** is executed at steps **1202** and **1204** to determine if a user is in proximity to the secured device in response to inputs received from the proximity sensor **116** as filtered by sensitivity module **602**. If a user is not in the vicinity of the secured device then that information is stored in the log file **318**, together with a time stamp indicating at which time the information is being stored, and the routine continues the polling and testing steps of **1204** and **1202**. If a user is determined to be in the vicinity of the secured device at step **1202** then that information is stored to log file **318**, together with the time stamp, and at step **1206**, information identifying the video program being displayed or computer program being used is stored to the log file **318**, together with the time stamp. In the case of a video program, the information stored to the log file is preferably an identification code, referred to herein as a display stream ID, which is transmitted with the video program. In the case of an executable computer program, the identification code stored to the log file is preferably a registry code or identifier, such as used to identify application programs by the operating system. In the case of the programs or data downloaded from remote sites, such as from the Internet or commercial databases, the information stored to the log file can be a Universal Resource Locator (URL) such as used to identify the source of information on the World Wide Web (WEB) or other similar type identification type information.

At step **1208** a test is performed if an exit command has been received to exit the routine. Such a command may be received from the secured device itself by way of a command entered via an input device, from a remotely located system operator or from a timer indicating either a particular predetermined time at which the routine should be terminated or expiration of a predetermined amount of time.

It is to be understood that the specific mechanisms and techniques, discussed herein are merely illustrative of exem-

plary applications of the principles of the invention. Numerous modifications may be made to the methods and apparatus described without departing from the true spirit and scope of the invention.

What is claimed is:

1. A controller for a security system which protects against unauthorized use of an electronic device comprising:

a control unit which receives a proximity input indicative of proximity of an individual to said electronic device, said control unit comprising,

arming means, responsive to said proximity input and to a timer input, for arming said security system a first changeable amount of time after said proximity input indicates cessation of activity at said electronic device; and

disarming means, responsive to said proximity input and to said timer input, for engaging an alarm, when said security system is armed, a second changeable amount of time after said proximity input indicates activity at said electronic device, if said security system is not disarmed within said second changeable amount of time; and

a command unit which causes removal of information from a visual display of said electronic device upon arming of said security system.

2. A controller as set forth in claim 1 wherein said removal of information from said visual display is removed in a manner selectable by an authorized user of said electronic device.

3. A controller as set forth in claim 1 wherein said proximity input is generated by a movement type sensor which detects movement.

4. A controller as set forth in claim 1 wherein said proximity input is generated by an image recognition program which receives a video input from a camera positioned to record visual images of a predetermined area around said electronic device, said image recognition program generating said proximity input upon detection of an unauthorized user attempting use of said device.

5. A controller as set forth in claim 1 wherein said control unit further comprises a voice recognition module which recognizes audio inputs generated by an authorized user of said device to control operation of said device.

6. A controller as set forth in claim 1 wherein said control unit further comprises a sensitivity module which responds to authorized user inputs to control sensitivity of sensors coupled to said security system.

7. A controller as set forth in claim 1 wherein said control unit further comprises a networking module which controls communications between said security system and remote devices.

8. A controller as set forth in claim 1 wherein said control unit further comprises a remote control module which receives commands from an authorized operator at a remote device to control operation of said security system.

9. A controller as set forth in claim 1 wherein said command unit further responds to arming of said security system by causing said electronic device to enter a power reduction mode.

10. A controller as set forth in claim 1 wherein said command unit responds to unauthorized use of said electronic device by capturing video information regarding said unauthorized use.

11. A controller as set forth in claim 1 wherein said command unit responds to unauthorized use of said electronic device by further capturing audio information regarding said unauthorized use.

12. A controller as set forth in claim 1 wherein said command unit causes removal of information from said visual display by invoking a resident security application.

13. A controller as set forth in claim 12 wherein said resident security application is a screen saver program.

14. A controller as set forth in claim 12 wherein said resident security application is stored externally to said device and is transmitted to said device upon receipt of a request from said device.

15. A controller as set forth in claim 1 wherein said command unit responds to unauthorized use of said electronic device by causing transmission over a local area type network of a signal indicating said unauthorized use.

16. A controller as set forth in claim 1 wherein said command unit responds to unauthorized use of said electronic device by causing input devices coupled to said electronic device to be disabled from accepting all inputs other than an authorized input.

17. A controller as set forth in claim 1 wherein said command unit responds to unauthorized use of said electronic device by causing data stored in said electronic device to be duplicated to a different storage device.

18. A controller as set forth in claim 1 further comprising a communication module which causes status information to be transmitted to a remote device.

19. A controller as set forth in claim 1 further comprising a reporting module which causes proximity information, indicative of information received from said proximity input, to be stored to a log file.

20. A controller as set forth in claim 19 wherein the reporting module further stores time stamp information to said log file.

21. A controller as set forth in claim 20 wherein the reporting module further stores information regarding the contents of said display when said system is armed.

22. A controller as set forth in claim 21 wherein the reporting module further stores information regarding the input received by input devices coupled to said electronic device in response to activation of said alarm and which stores information transmitted by said electronic device to output devices coupled to said electronic device.

23. A controller as set forth in claim 22 further comprising a dynamic response module which changes response of said control unit to said proximity input as a function of said information stored in said log file.

24. A proximity sensing system which senses activity in the vicinity of a computerized device, comprising:

an activity detector which responds to an activity signal, indicative of activity in the vicinity of the computerized device, by storing information indicative of said activity to a log file; and

an input device detector, responsive to said activity detector, which stores information indicative of inputs entered into said computerized device to said log file.

25. A usage tracking system for a computerized electronic device which includes an output device for outputting user viewable information, the usage tracking system comprising:

a proximity detector which responds to an activity signal indicative of activity in the vicinity of said computerized electronic device by storing information indicative of said activity signal to a log file; and

a content detector, responsive to said proximity detector, which stores information indicative of said user viewable information being outputted by said output device to said log file.

* * * * *

US006137480A

United States Patent [19]

Shintani

[11] Patent Number: 6,137,480

[45] Date of Patent: Oct. 24, 2000

[54] **COMPUTER SYSTEM USING A PORTABLE CARD FOR MANAGING SECURITY AND POWER-SAVING FEATURES**

[75] Inventor: **Peter Shintani**, Tokyo, Japan

[73] Assignee: **Sony Corporation**, Tokyo, Japan

[21] Appl. No.: **08/995,411**

[22] Filed: **Dec. 19, 1997**

[30] **Foreign Application Priority Data**

Dec. 27, 1996 [JP] Japan 8-351162

[51] **Int. Cl.**[7] **G09G 5/00**; G08C 21/00; G08B 1/08

[52] **U.S. Cl.** **345/169**; 178/18.04; 178/18.09; 340/825.31

[58] **Field of Search** 345/162, 169, 345/172; 340/825.31; 705/18; 235/380, 382, 382.5, 492, 493; 713/200, 201, 202, 320, 324; 178/18.01, 18.03, 18.04, 18.09, 18.1

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,377,269	12/1994	Heptig et al.	340/825.31
5,379,033	1/1995	Fujii et al.	340/825.31
5,382,778	1/1995	Takahira et al.	235/382
5,698,837	12/1997	Furuta	235/492
5,821,854	10/1998	Dorinski et al.	340/825.31
5,841,868	11/1998	Helbig, Sr.	340/825.31

Primary Examiner—Vijay Shankar

Attorney, Agent, or Firm—Jay H. Maioli

[57] **ABSTRACT**

To enhance service to a user and the security and others of a computer system by managing the respective operations of plural computer terminals using a non-contact card, a user is authenticated by a communicating between the non-contact card storing the personal identification information of the user and peripheral equipment arranged in the vicinity of the user such that login to a computer is automatically executed according to the result of the authentication. By making communication with the non-contact card periodically it is determined whether the user has temporarily left his/her seat, in which case a screen saver is activated and a file is automatically stored.

11 Claims, 3 Drawing Sheets

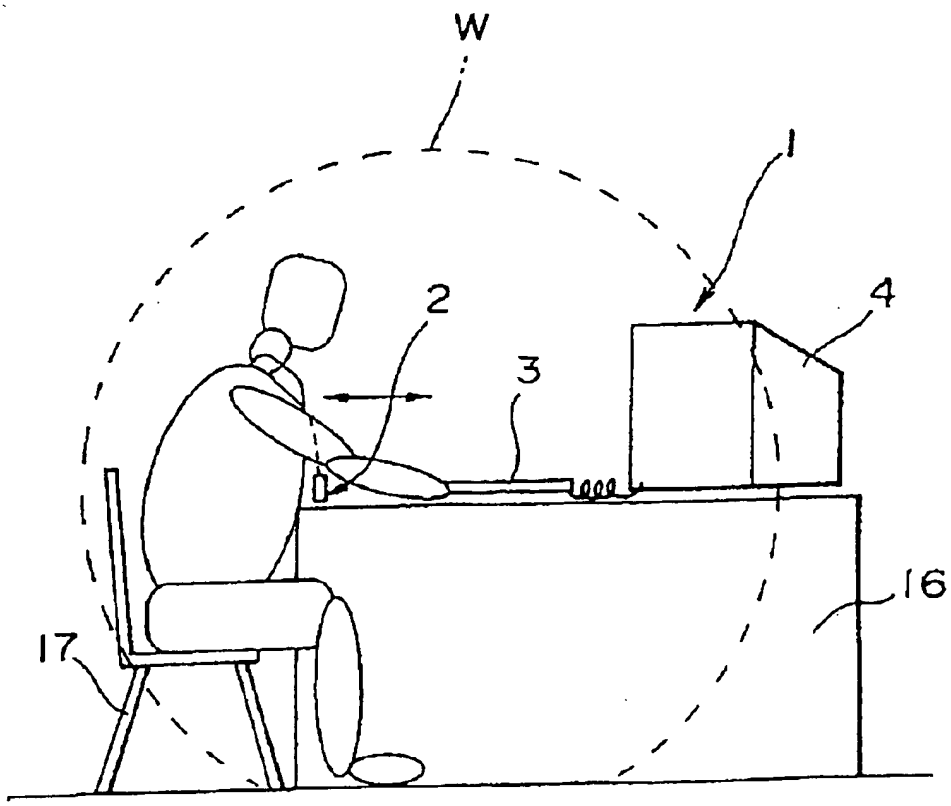
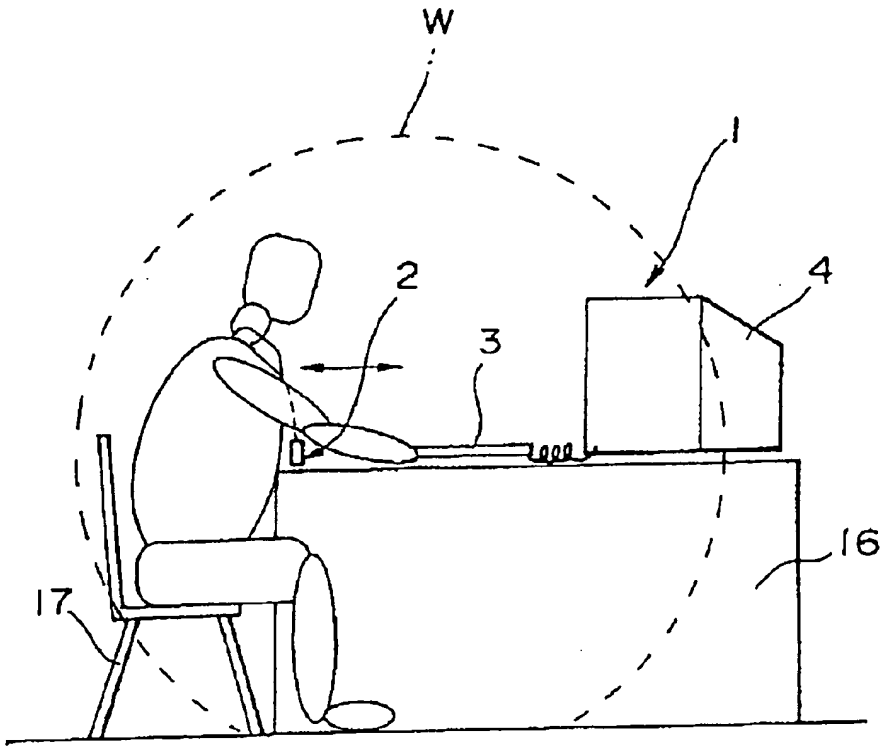


FIG. 1



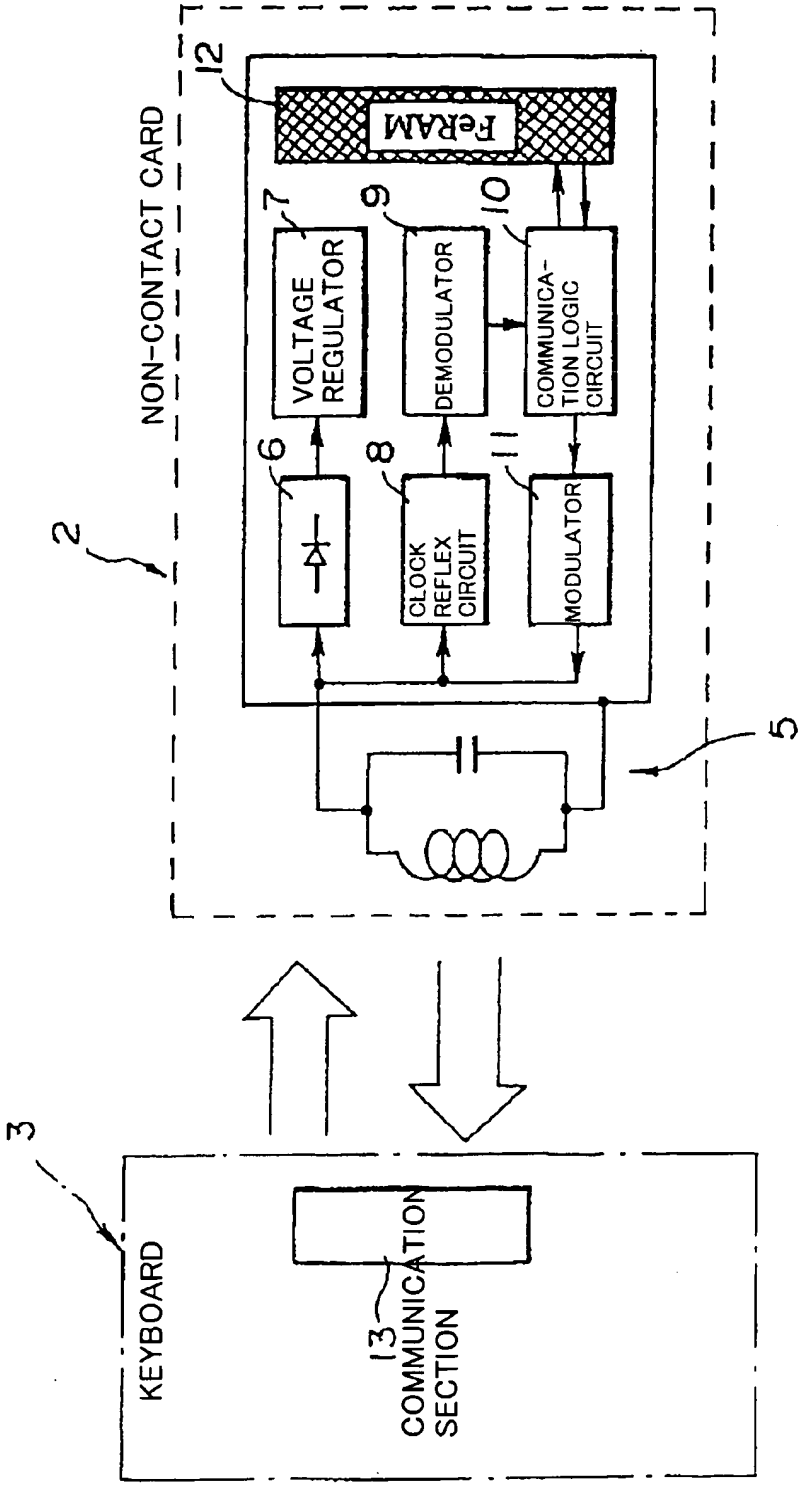
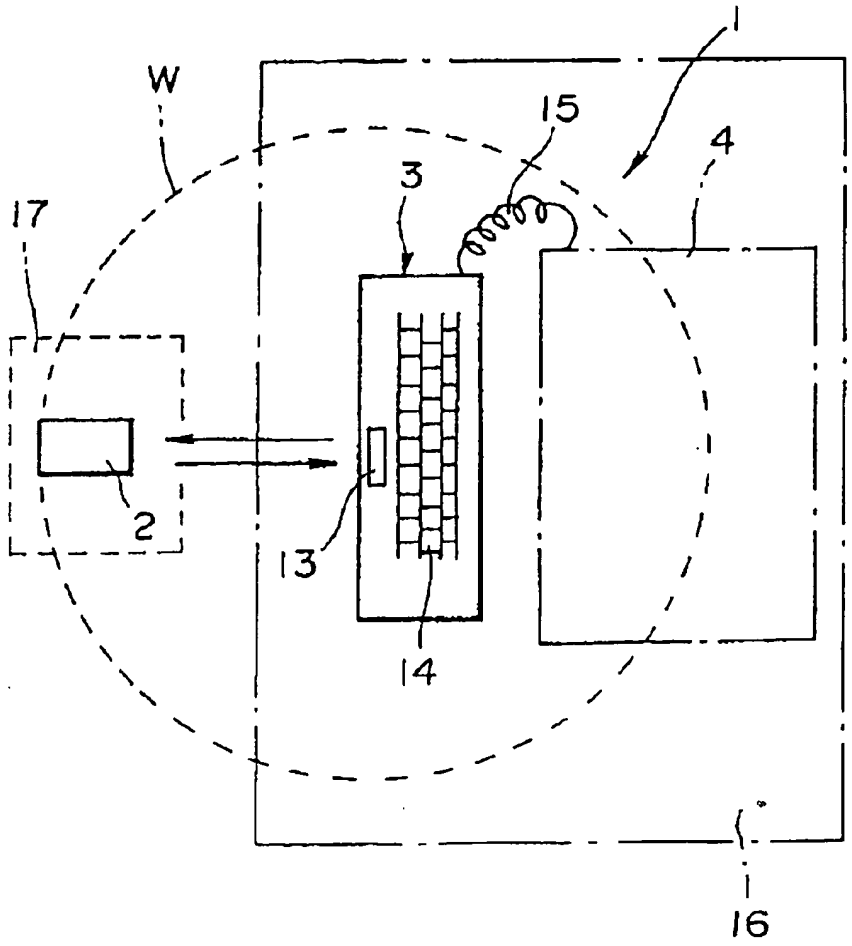

NON-CONTACT CARD
12
FeRAM
7
VOLTAGE REGULATOR
9
DEMODULATOR
10
COMMUNICATION LOGIC CIRCUIT
6
8
11
CLOCK REFLEX CIRCUIT
MODULATOR
2
5
3
KEYBOARD
13
COMMUNICATION SECTION

FIG. 2

FIG. 3



COMPUTER SYSTEM USING A PORTABLE CARD FOR MANAGING SECURITY AND POWER-SAVING FEATURES

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to a computer system for managing a computer terminal using a non-contact card and enables exact communication between the non-contact card and the computer terminal.

2. Description of the Related Art

In a conventional type computer system, as a means for preventing data or a file as a work object from being lost when a computer is disabled suddenly, a file automatic storage function included in the word processor software for example is known. The file automatic storage function periodically and automatically stores a file as a work object in a storage medium and enables return to a work state before a predetermined time has expired even if a computer is disabled.

If a user of a computer does not use the computer for a long time and the same video signal continues to be displayed on a computer display, a CRT display screen seizes. As a means for preventing the above situation, a screen saver and a power saving function are known.

The above screen saver is software for preventing a CRT display screen from locally seizing by detecting that a computer is not used for predetermined time, automatically generating a graphic image and displaying it on the display.

The above power saving function automatically changes the current state of a computer to a standby state or darkens the screen by detecting that no video signal has been supplied from the body of the computer to a computer display for a predetermined time.

However, the above file automatic storage function is executed independent of whether a user is actually sitting in front of a computer terminal or not and if a user is leaving his/her seat and another person uses a computer as the person likes, the result of the operation is stored.

The screen saver and the power saving function are devised to prevent a computer CRT display screen from seizing but, are not devised to prevent another person except a real user from operating a computer terminal and another person can readily utilize a computer terminal.

One proposed approach is enabled by setting a password that when a real user is absent, another person cannot utilize the computer terminal of the real user, however, the real user is required to input his/her password every time the real user returns to his/her seat again and it is troublesome.

SUMMARY OF THE INVENTION

The present invention is made to solve the above problems and a computer system according to the present invention is constituted by a portable card provided with a communication circuit for storing the personal identification information of a user and communication means provided to peripheral equipment constituting the computer system for communicating with the above portable card and is characterized in that a computer processes the above personal identification information received from the portable card via the communication means.

As the communication means for communicating with a non-contact card which is excellent in portability is provided to peripheral equipment arranged in the vicinity of a user of a computer terminal according to the present invention, the non-contact card suspended from a user's neck, for example, is in the range of the communicable area of the communication means if the user sits down and a secure detection area can be acquired.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is an explanatory drawing showing relationship between terminal equipment according to the present invention and a user having a keyboard;

FIG. **2** is an explanatory drawing showing the structure of a non-contact card according to the present invention in block diagram; and

FIG. **3** is an explanatory drawing showing the non-contact card brought close to a desk and a detection area by the keyboard provided with a detecting section for detecting the non-contact card.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Next, referring to the drawings, a computer system according to the present invention will be described.

The computer system according to the present invention is constituted by a computer terminal **1** and a portable non-contact card **2** which can be used with the portable non-contact card suspended from the neck and others of a user who operates the computer terminal **1** as shown in FIG. **1**. The computer terminal **1** is constituted by a keyboard **3**, which is the input means, and a display **4**. The body of the computer and other elements are not shown.

The non-contact card **2** is constituted by a resonance circuit **6** consisting of a coil and a capacitor, a rectifier **7** connected to the resonance circuit **6**, a voltage regulator **8** connected to the rectifier **7** for generating supply voltage in the non-contact card, a clock regenerating circuit **9**, a demodulator **10**, a microcomputer **11**, a modulator **12** and nonvolatile memory FeRAM **13** as shown in FIG. **2**.

Personal identification information is written to the nonvolatile memory FeRAM **13** and at least a password proper to an individual and a code for guaranteeing identity are included in the personal identification information and further information, such as accessible file name and data type in a usable computer system is also written.

A communication section **14** for communicating with the non-contact card **2** is provided to the keyboard **3** in addition to operating keys **18** as shown in FIGS. **2** and **3**.

The communication section **14** is arranged suitably, for example on the side face and others opposite to the user side of the keyboard so that it does not hinder the operation of arranged keys. Information received by the communication section **14** is transmitted together with data input via the keys **18** to the body of the computer **5** via a cable **15** and the display **4**.

Information may be also transmitted between the keyboard **3** and the display **4** not via the cable **15** but by wireless transmission. Information may be also transmitted between the display **4** and the body of the computer **5** not via the cable but by wireless.

When the communication section **14** constituted as described above detects the non-contact card **2**, personal identification information stored in the non-contact card **2** is transmitted to the communication section **14**, is supplied to the body of the computer via the cable **15** and the display **4**, and the body of the computer authenticates a user. A user table is stored on a storage medium such as a hard disk and

memory of the body of the computer. The personal identification information of at least one user accessible to the body of the computer is stored in the user table.

Therefore, the body of the computer authenticates by comparing stored personal identification information and personal identification information received from the non-contact card **2**. Personal identification information is transmitted from the keyboard **3** to the body of the computer according to the same format as data input via the keys of the keyboard **3**.

If personal identification information transmitted from the non-contact card **2** is authenticated by the body of the computer and the body of the computer judges that the owner of the non-contact card is a real user, login for access to the body of the computer and for access to a network connected to the body of the computer is automatically executed. In the meantime, if as a result of the authentication, the body of the computer judges that the owner of the non-contact card is an invalid user, a message reporting the above is displayed on the display **4** and login for access to the body of the computer and the network is not executed.

When a user starts the operation of a predetermined file or predetermined data, it is determined whether the above user is provided with access authority to the predetermined file or data. That is, if the body of the computer accepts an instruction by a user to start the operation of a new file or new data, a command to transmit the information of an accessible file name or data type stored in the non-contact card **2** is output to the non-contact card **2** via the display **4** and the keyboard **3**. In the non-contact card **2**, the microcomputer **11** recognizes the command received via the clock regenerating circuit **9** and the demodulator **10**, reads the information of the file name or data type stored in FeRAM **13** to which the user can access and outputs the information to the modulator **12**. As described above, the information of the file name or data type to which the user can access is modulated and transmitted to the body of the computer via the communication section **14** of the keyboard **3** and the display **4**. The body of the computer compares the transmitted information of the file name or data type to which the user can access and the file name or data of which the user instructs to start the operation. If the result of the comparison coincides, the body of the computer allows access to the file or data of which the user instructs to start the operation and if the result of the comparison does not coincide, the body of the computer instructs the display **4** to display a message reporting that the access is disabled.

Communication between the non-contact card **2** and the communication section **14** is executed every predetermined time, for example every 30 seconds, so that if a user temporarily leaves his/her seat at work, communication between the communication section **14** and the non-contact card **2** is disabled. The body of the computer detects the above state in which communication is disabled, stores a file or data at work and inhibits the change of the file or data at work until the user returns to his/her seat and communication between the communication section **14** and the non-contact card **12** is enabled again. Further, the body of the computer executes processing for a power saving mode such as activating a screen saver to prevent the CRT display **4** from seizing, darkening the screen of the display and stopping the rotation of a hard disk. When the user returns to his/her seat and communication between the communication section **14** and the non-contact card **2** is restarted, the body of the computer enables the update of the file or data at work, executes processing for releasing the power saving mode such as the termination of the screen saver and lightening the screen of the display **4** and returns the current state to a state in which operation is enabled.

An area provided to the keyboard **3** in which the communication section **13** can communicate is limited to a fixed range W shown in FIGS. **1** and **3** and in this embodiment in which the communication section **13** is provided to the keyboard **3**, the above area is limited to the spherical area W with the keyboard **3** as the center.

The non-contact card **2** suspended from the neck, for example, of a user is automatically located in the vicinity of the keyboard **3** by setting a communicable area as described above if the user sits on a chair **17**, for example to use the computer terminal **1** on the table **16** as shown in FIG. **1**, that is, in the communicable area W of the communication section **13** provided to the keyboard **3**.

Even if a position in which a user works and the body of the computer **5** are separated, the keyboard **3** is normally located close to a user and as a result, located in the communicable area W.

For example, even in a room in which plural computer terminals **1** are arranged, communication between the non-contact card **2** and the computer terminal **1** is enabled in units of user by providing the communication section **14** with the non-contact card **2** to the peripheral equipment connected to the body of the computer **5** and arranged in the vicinity of a user and suitably setting a communicable area W as described above and radio interference between plural non-contact cards **2** and plural computer terminals **1** can be prevented.

If a detected state is bad, the non-contact card **2** has only to approach the keyboard **3** suitably and special adjustments and the like are not required.

In this embodiment, the communication section **14** is provided to the keyboard **3**, however, the communication section has only to be provided to the peripheral equipment connected to the body of the computer and arranged in the vicinity of a user and it need scarcely be said that the communication section may be also provided to a mouse, a display, a microphone used for the input of voice, a microphone stand, or an external storage such as a magneto-optical disc.

According to the computer system described above, when a user sits on a chair before which a computer terminal is installed, the user is automatically authenticated and login to the body of the computer and a network is executed.

Further, if a user suspends work and leaves his/her seat, that is, goes out of the detection area W, it is judged that work is suspended and security can be kept by darkening the screen of the display **4**, automatically saving a file at work and others. If a message telling that work is continued is displayed on the screen, reported in voice or both, in this state if another user tries to access that person is prevented from interfering during work and security can be kept. It can be also managed when a user starts to work.

The present invention is not limited to the above embodiment and various variations are allowed. For example, in the above embodiment, when a user sits on a chair, a computer automatically authenticates the user and executes login, however, a computer may also require a user to input his/her password only when power is applied in consideration of further security. Also, in the above embodiment, information such as an accessible file name and an accessible data type in a computer system is written to a non-contact card, however, accessible file name and data type may be also stored in the hard disk and others of the body of the

computer with them and the identification information of a user in pairs. In this case, if the body of the computer accepts an instruction by a user to start the operation of a new file or new data, the body of the computer compares the personal identification information of a user stored with the personal identification information and accessible file name, data type and others stored in the body of the computer in pairs and the personal identification information received to the non-contact card **2** and if they coincides, the body of the computer allows access to the file or the data.

Further, in the above description of the present invention, the computer is a desktop computer, however, the present invention can be also applied to a portable computer.

As described above, in a computer system according to the present invention, a communication section for communicating with a non-contact card which is excellent in portability is provided to peripheral equipment arranged in the vicinity of a user of a computer terminal, preferably, if a communication section is provided to mobile equipment such as a keyboard and a mouse, the non-contact card **2** suspended from his/her neck and others is automatically located in the vicinity of the keyboard **3** when a user sits on a chair, that is, located in the communicable area W of the communication section **14** provided to the keyboard **3** and a secure detection area can be acquired.

Also, even if a user temporarily leaves his/her seat because communication is periodically made even while the user works, the security of a file and data at work can be kept.

What is claimed is:

1. A computer system constituted by an information processing section and peripheral equipment including at least a display and a keyboard, comprising:

a portable card including a communication circuit for storing personal identification information of a user; and

communication means included in said peripheral equipment for communicating with said portable card, wherein said information processing section:

processes said personal identification information received from said portable card via said communication means,

activates a screen saver when communication between said portable card and said communication means is interrupted, and

terminates the screen saver when communication is restarted between said communication means and said portable card storing the personal identification information of the user for whom login was executed before the communication was interrupted.

2. The computer system according to claim **1**, wherein

said information processing section stores a user table identifying users for whom login to said computer is allowed; and

said information processing section authenticates a user by comparing said personal identification information received from said portable card and said user table.

3. The computer system according to claim **2**, wherein said information processing section automatically executes login when it is judged that said personal identification information received from said portable card is included in said user table.

4. The computer system according to claim **2**, wherein said information processing section instructs said display to display a message that login is not allowed when it is judged that said personal identification information received from said portable card is not included in said user table.

5. The computer system according to claim **1**, wherein said portable card includes means for communicating between said portable card and said communication means every predetermined period.

6. The computer system according to claim **5**, wherein said information processing section automatically stores data at work when communication between said portable card and said communication means is interrupted.

7. The computer system according to claim **1**, wherein said information processing section automatically stores data at work when communication between said portable card and said communication means is interrupted.

8. The computer system according to claim **5**, wherein said information processing section changes the current mode to a power saving mode when communication between said portable card and said communication means is interrupted.

9. The computer system according to claim **5**, wherein said information processing section inhibits input of data from said keyboard until communication between said portable card storing the personal identification information of the user for whom login is executed before the communication is interrupted and said communication means is restarted when the communication between said portable card and said communication means is interrupted.

10. The computer system according to claim **5**, wherein said information processing section enables input and change of data when communication between said portable card storing the personal identification information of the user for whom login is executed before the communication is interrupted and said communication means is restarted after the communication between said portable card and said communication means is interrupted.

11. The computer system according to claim **5**, wherein said information processing section releases a power saving mode if communication between said portable card storing the personal identification information of the user for whom login is executed before the communication is interrupted and said communication means is restarted after the communication between said portable card and said communication means is interrupted.

* * * * *

US005335168A

United States Patent [19]

Walker

[11] Patent Number: 5,335,168

[45] Date of Patent: Aug. 2, 1994

[54] COMPUTER SYSTEM WITH POWER-DOWN MODE FOR MONITOR

[75] Inventor: Richard E. Walker, The Woodlands, Tex.

[73] Assignee: Compaq Computer Corporation, Houston, Tex.

[21] Appl. No.: 4,144

[22] Filed: Jan. 13, 1993

[51] Int. Cl.[5] G06F 1/00

[52] U.S. Cl. 364/707; 364/242; 364/273; 364/DIG. 1

[58] Field of Search 395/750; 364/231, 242, 364/273.1, 707

[56] References Cited

U.S. PATENT DOCUMENTS

4,980,836	12/1990	Carter	364/483
5,021,983	6/1991	Nguyen et al.	364/707
5,167,024	11/1992	Smith et al.	364/273.1
5,237,692	8/1993	Raash et al.	364/273.1

OTHER PUBLICATIONS

PC Week Feb. 11, 1991 v8 n6 p. 5(1) PS/2 L40SX packs design novelties . . . author Michael Caton.

EDGE: Work-Group Computing Report Mar. 18, 1991 v2 n43 p. 28(1) Notebook displays . . . author Phoenix Technologies Ltd (Product Anouncement).

PC Computing, Oct. 1993 p. 297 Nanao USA Corporation.

NUTEK Specification 803299/92-93, Dec. 3, 1992, pp. 1-2.

"Auto turn-off monitors," Nutek, 1992, pp. 1-4.

"Environmental Labelling of Display Units," Presented at Third International Scientific Conference, Sep. 1992, pp. 1-4.

Primary Examiner—Jack B. Harvey

Assistant Examiner—Craig Steven Miller

Attorney, Agent, or Firm—L. Jon Lindsay

[57] ABSTRACT

A computer system has a monitor which can be powered down to conserve electrical power. The Monitor has two power modes, normal power mode and low power mode. Upon receiving a signal from the CPU, the monitor switches between power modes.

14 Claims, 2 Drawing Sheets

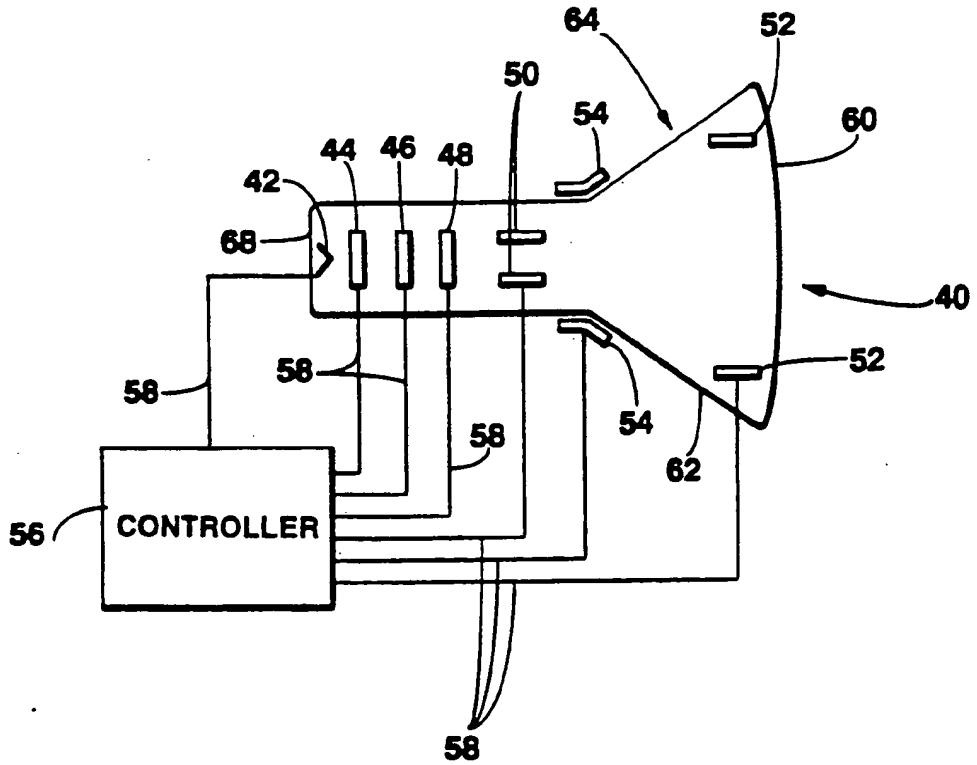
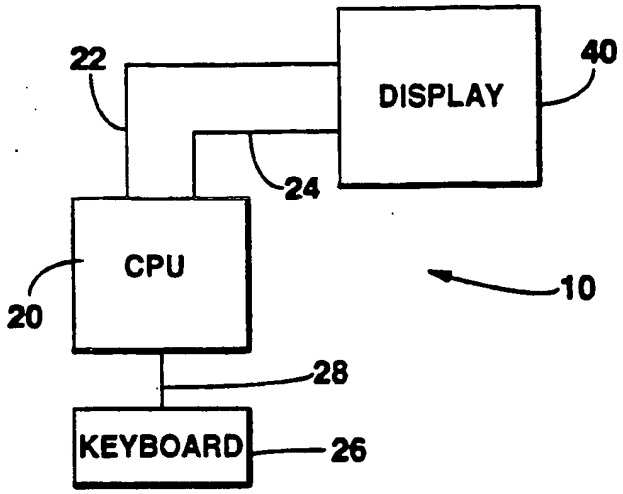


Fig. 1


22
DISPLAY
40
24
CPU
20
10
28
KEYBOARD
26

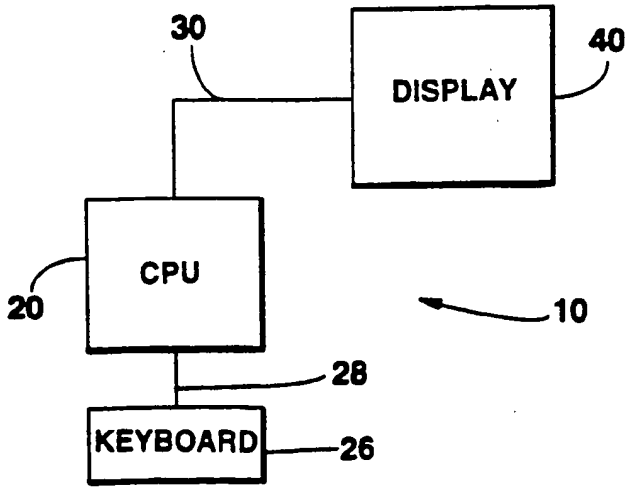

30
DISPLAY
40
CPU
20
10
28
KEYBOARD
26

Fig. 2

Fig. 3

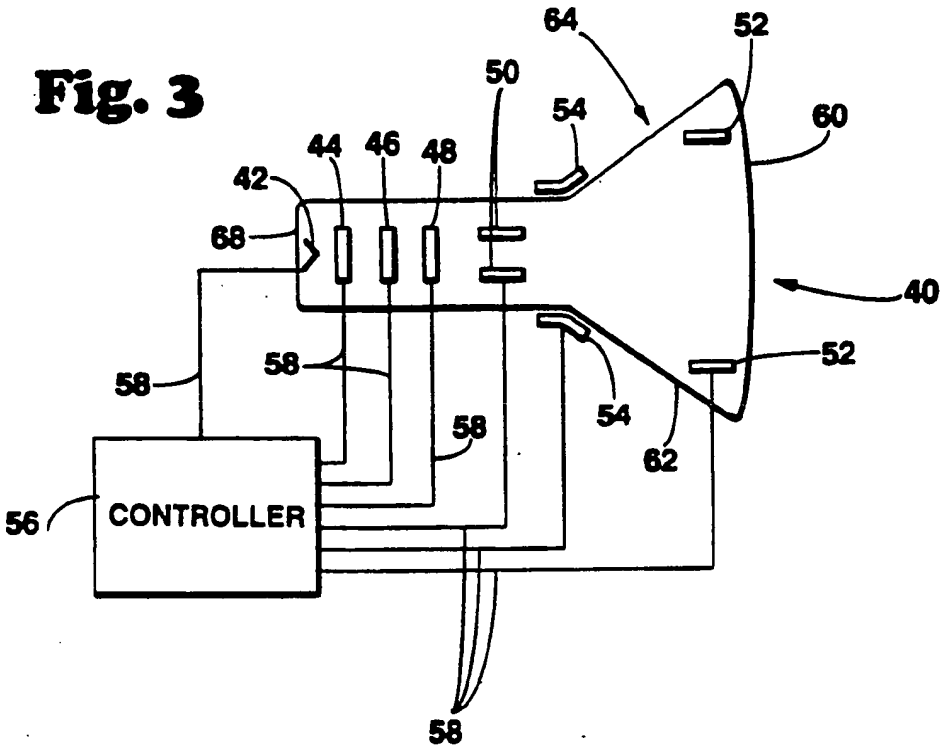


Fig. 4

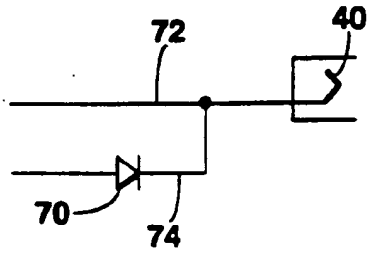
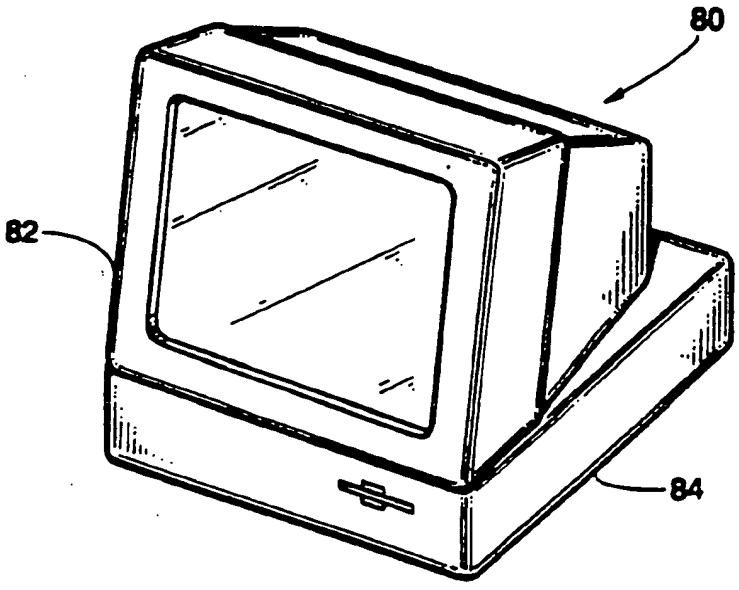


Fig. 5



COMPUTER SYSTEM WITH POWER-DOWN MODE FOR MONITOR

BACKGROUND OF THE INVENTION

This invention relates to power management and power conservation techniques for personal computers. More particularly, this invention relates to power conservation in the monitor of a personal computer system.

In recent years, power management features in personal computers have come into more and more common use, particularly in the very small, battery operated notebook computers. An example of an apparatus for reducing power consumption in a computer system is shown in U.S. Pat. No. 4,980,836, which is assigned to the assignee of the present invention and incorporated herein by reference. This apparatus shuts down part of the computer system after a period of inactivity, thus conserving electrical power.

Other ways of reducing power consumption may involve turning off, or slowing down, only certain internal peripheral devices, such as the hard drive. Usually, these methods monitor activity to the peripheral device and, after a certain period of inactivity, shut the peripheral down. Typical power conservation for powering down a hard drive may result in approximately a three percent reduction in power usage by the entire computer system.

In most personal computer systems, the monitor is one of the biggest users of power. However, no one has yet found a way to provide power management features in a computer monitor such as the cathode ray tube (CRT) monitors commonly used with most desk top personal computers. These monitors are turned on all the time the computer is in use and draw full power the entire time. In a typical system, the monitor may consume three-fourths of all the power. Therefore, considerable power savings may be had if some way to power down the monitor could be accomplished.

In a typical CRT monitor, a filament produces electrons when it becomes very hot. A series of grids and anodes strips the electrons from the filament, accelerates the electrons into a beam and focuses the beam onto a phosphorescent screen. A set of coils deflects the beam onto different areas of the screen to produce an image. The filament, the grids and a first anode form an electron gun. A first grid modulates the number of electrons in the electron beam. A second grid accelerates the electrons through the electron gun. A third grid focuses the electron beam very tightly. The first anode accelerates the electrons even more before they leave the electron gun. Then the coils deflect the beam in the horizontal and vertical directions. Finally, a second anode, a very high voltage device, accelerates the beam a final time before the electrons strike the phosphors on the screen causing an emission of photons. Control circuitry provides the control signals to synchronize the operation of each of these elements so that an image appears on the screen. The deflection coils and the second anode are by far the biggest drain on the power supply.

When a user turns on a monitor, there is usually a several second delay before an image appears on the screen. This delay is due to the need to heat up the heating filament of the electron gun. Although, the deflection coils and the second anode draw the most power, they can be turned on much more quickly than can the heating element. The monitor's control circuitry and the electron gun, except for the filament, can also be turned on very quickly. Therefore, the limiting factor in turning on a monitor is the time needed to heat up the heating filament.

Additionally, the limiting factor in the useful life of a CRT monitor is usually the heating filament. In other words, keeping the filament hot will eventually cause the filament to wear out, usually before the other elements of the monitor wear out. The ratio of the life of the filament to its temperature is governed by the root mean square distribution. Thus, an increase in the life of a filament will not be linearly proportional to a reduction in the temperature of the filament. Instead, the increase in the life of the filament will be proportional to the square of the reduction in its temperature, so a relatively small change in the temperature of the filament will result in a relatively large change in its useful life. Also, the ratio of the change in voltage across the filament to the change in temperature of the filament is governed by the root mean square distribution. In this case, the change in voltage is proportional to the square of the change in temperature. Therefore, a reduction in the voltage across the filament will result in a relatively small reduction in the temperature of the filament, which will result in a relatively large increase in its useful life.

Televisions made several years ago powered down every part of the television system when the television was turned off. Then when the television was turned on, several seconds would pass before an image would appear on the screen, because the system had to wait for the heating element to heat up. However, most televisions made today only require a short wait before an image appears. This short time period is due to the fact that most televisions no longer power down every element of the system when the television is turned off. Instead, the new televisions keep the heating element hot even when the system is off. Thus, if a person were to touch the back of a modern television, that person would find the television to be quite warm even though it had been left off for several hours.

Many screen-saver programs already exist for personal computers. These programs usually remove the image on the screen of the monitor after a period of user inactivity and replace the image with a moving image that will not "burn" into screen. One type of screen-saver blanks the screen entirely, so that there is no image at all. When the user touches a key on the keyboard or moves a mouse pointer, thus resuming activity, the previous image is restored to the screen. However, screen-saver programs do not actually conserve any power in the system. Instead, all of the elements of the monitor remain under full power, even if the screen has been completely blanked out.

Therefore, it is an object of the present invention to provide a power management feature for a personal computer system by powering down selected parts of the system's monitor.

BRIEF SUMMARY OF THE INVENTION

It is an object of the present invention to provide a computer system capable of reducing the power consumption of its display device.

It is a further object to provide a computer display device having a reduced power mode for conserving electrical power.

A standard CRT monitor has several elements that consume power. The present invention powers down some or all of these elements in order to conserve power.

The primary elements of a standard CRT monitor for a computer system include a heating filament, control circuitry, a modulator grid, an accelerator grid, a focusing grid, a first accelerating anode, a second accelerating anode, and deflection coils. The invention changes the monitor's power consumption from a normal power mode to a low power mode by turning off the power to all of these elements except the heating filament. The power to the heating filament may remain fully on or slightly reduced.

The computer system sends signals to the monitor to enter the low power mode and subsequently to resume the normal power mode. The signal to enter the low power mode is generated after a period of user inactivity. Thus, the invention monitors the time from the last input from the user through any input device. The signal to resume the normal power mode, on the other hand, is generated by any user activity through any input device.

DESCRIPTION OF THE DRAWINGS

FIG. 1 is a block diagram of a computer system with separate on/off signal wires,

FIG. 2 is a block diagram of a computer system with the on/off signals encoded in the video signals.

FIG. 3 is diagram of a computer monitor,

FIG. 4 is a schematic diagram of a circuit for providing alternate voltages to a heating filament according to the present invention.

FIG. 5 is a perspective view of a computer system incorporating a captive monitor,

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

A computer system 10 incorporating the present invention is shown in FIG. 1. The computer system 10 has a CPU 20, a keyboard 26 and a monitor 40. Keyboard signal wires 28 connect the keyboard 26 to the CPU 20. Monitor control signal wires 22 connect the monitor 40 with the CPU 20. Power mode signal wires 24 send the power mode signals to the monitor 40 from the CPU 20.

A second embodiment of the computer system 10 incorporating the present invention is shown in FIG. 2. This computer system 10 has a CPU 20, a keyboard 26 and a monitor 40. Keyboard signal wires 28 connect the keyboard 26 to the CPU 20. Monitor control signal wires 30 with encoded power mode signals connect the CPU 20 with the monitor 40.

FIG. 3 shows the elements of a monitor 40 for use in the present invention. The housing 62 of the CRT 64 has a screen 60 and within the housing 62 are the power-consuming elements such as the heating filament 42, modulator grid 44, accelerator grid 46, focusing grid 48, first anode 50, second anode 52 and deflector coils 54. Control Circuitry 56 controls the operation of these elements through control wires 58.

The present invention reduces the power consumption of a computer system by turning the power off to selected elements in the monitor. Thus, the system has two power modes when it is powered-on, a low powered-on mode and a normal powered-on mode. In the preferred embodiment, electrical power is turned off to all of the power-consuming elements except the heating filament 42 when the system is in the low powered-on mode. In this mode, the power to the heating filament 42 remains high, but is reduced slightly. Thus, the system has a normal powered-on mode in which the power-consuming elements are all turned on and a low powered-on mode in which the selected elements are turned off.

In another embodiment of the invention, the power to the heating filament 42 remains the same, even in the low powered-on mode. In still another embodiment, the power to the heating filament 42 is turned off along with the power to the other power-consuming elements of the monitor 40 in the low powered-on mode.

This invention achieves a 65–70% reduction in the power consumption by the computer system. By comparison, powering down the hard drive of a personal computer system may achieve only a 3% reduction in power consumption by the computer system.

This invention has particular application in a computer system wherein the monitor, or display device, is an integral part of the system, i.e. the display device is "captive" within the system as shown in FIG. 5. Such a captive-monitor computer system may have a computer system 80 with a monitor 82 built onto the CPU housing 84. Many portable computer systems and personal word-processing systems incorporate a captive monitor subsystem without which the system cannot operate. By contrast, a computer system with a non-captive monitor is such that any monitor can be plugged into a monitor jack in the side of the CPU box of the system. Previously, there have been no monitors with power-down features; thus, a captive-monitor system is ideal for the present invention, since the monitor and the CPU must work in special cooperation to power-down the monitor.

In the present invention a signal is sent to the monitor 40 from the CPU system 20 commanding the monitor 40 to power down the selected elements. In the preferred embodiment, this signal is encoded in the monitor control signals 30 in FIG. 2. The monitor control signals 30 include red-green-blue (RGB) video signals and horizontal and vertical sync signals. The sync signals are turned off, or brought to zero, thus signaling the monitor to turn off the selected elements. Control circuitry 56 (FIG. 3) in the monitor 40 detects whether the sync signals are off and then turns off the selected elements through control wires 58 in response thereto. Then when the sync signals are turned back on, the control circuitry 56 turns the selected elements back on.

In the foregoing preferred embodiment, the RGB video signals are not turned off. However, in another embodiment, these signals are used to command the monitor 40 to turn off the heating filament 42 in addition to the other selected power-consuming elements, effectively turning off the entire monitor 40 except for a small circuit in the control circuitry 56 that monitors the monitor control signals 30 in order to turn the monitor 40 back on. Thus, the monitor 40 can detect when the CPU box 20 has been turned off and can put itself into low power mode until the user turns the CPU box 20 back on.

A person skilled in the art will recognize that there are many ways to send the signals for commanding the monitor to turn the selected elements on and off. For example, in one embodiment, the timing of the sync signals may be changed, instead of sending the signals to zero. In another embodiment, separate power mode signal wires 24 (FIG. 1) are used to send the signals. In this embodiment, one wire carries a simple on/off sig-

nal. The person skilled in the art will recognize that this is not an all-inclusive list of the ways to send the signals.

In the preferred embodiment, the power to the heating filament **42** is slightly reduced. This power reduction adds additional power savings, but does not reduce the temperature of the filament **42** too much, so that the filament **42** can be returned to its normal operating temperature in approximately two seconds. In many monitors the normal operating voltage applied to the filament **42** is 6.3V. In the present invention, the voltage is reduced to approximately 5V. FIG. **4** shows the 6.3V source applied to the filament **42** through wire **72**. The 5V source is applied through diode **70** and wire **74** to the filament **42**. In this arrangement, when the 6.3V source is turned on, the diode **70** is reversed biased, so the filament **42** receives the 6.3V. When the control circuitry **56** receives the signal to put the monitor **40** in the low power mode, the 6.3V source is turned off, so the diode becomes forward biased and the 5V source is applied to the filament **42**. A person skilled in the art will recognize that the 5V source can come from any source. For example, in the embodiment shown in FIG. **1**, the 5V can come through the power mode signal wires **24** in a separate wire or as part of the on/off signal. In another embodiment, the 5V source may be a standby source within the power supply or control circuitry **56** of the monitor **40**.

What is claimed is:

1. A computer system having a central processing unit comprising:
- a display device having a normal powered-on mode and a low powered-on mode;
- a heating filament disposed within the display device;
- a normal voltage source applied to the heating filament when the display device is in the normal power mode;
- a low voltage source applied to the heating filament when the display device is in the low power mode; and
- means for changing the power mode of the display device between the normal powered-on mode and the low powered-on mode.

2. The computer system of claim **1** wherein the display device is a captive display device.

3. The computer system of claim **1** further comprising:
- means for generating a first signal;
- the means for changing the power mode being capable of changing the power mode in response to the first signal.

4. The computer system of claim **3** wherein the means for changing the power mode is capable of changing the power mode of the display device from the first power mode to the second power mode in response to the first signal.

5. The computer system of claim **4** further comprising:
- a means for generating a second signal;
- the means for changing the power mode being capable of changing the power mode of the display device from the second power mode to the first power mode in response to the second signal.

6. The computer system of claim **5** further comprising:
- an input device capable of generating an input signal; and
- a means for generating a time-out signal after a predetermined period of time has elapsed since the last input signal;
- the means for generating the first signal being capable of generating the first signal in response to the time-out signal.

7. The computer system of claim **6** wherein the means for generating the second signal is capable of generating the second signal in response to the input signal.

8. The computer system of claim **5** further comprising:
- an input device capable of generating an input signal;
- the means for generating the second signal being capable of generating the second signal in response to the input signal.

9. A method for reducing power consumption of a computer system comprising the steps of:
- providing a display device having a normal power consumption mode and a lower power consumption mode; and
- reducing the power to the display device from the normal power consumption mode to the lower power consumption mode by reducing the power to selected elements of the display device;
- wherein said power reducing step includes the additional steps of:
  - turning off the power to a first set of power-consuming elements of the display; and
  - reducing the power to a second set of power-consuming elements of the display.

10. The method of claim **9** wherein:
- the second set of power-consuming elements includes a heating filament;
- the display device includes a normal voltage source applied to the heating filament when the display device is in the normal power consumption mode; and
- the display device includes a low voltage source applied to the heating filament when the display device is in the lower power consumption mode.

11. The method of claim **9** comprising the further step of generating a first signal, whereby the step of reducing the power is responsive to the first signal.

12. The method of claim **11** comprising the further steps of:
- generating an input signal; and
- generating a time-out signal after a predetermined period of time after the last generated input signal;
- whereby the step of generating the first signal is responsive to the time-out signal.

13. A method of reducing power consumption of a display device having a normal power mode an a low power mode for use with a computer system comprising the steps of:
- receiving a first signal from the computer system; and
- reducing the power consumption of the display device from the normal power mode to the low power mode in response to the first signal by reducing the power to selected elements of the display device.

14. The method of claim **13** comprising the further steps of:
- receiving a second signal from the computer system; and
- increasing the power consumption of the display device from the low power mode to the normal power mode in response to the second signal.

* * * * *